#3

LAW OFFICES
SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20037-3213
TELEPHONE (202) 293-7060
FACSIMILE (202) 293-7860
www.sughrue.com

J. Frank Osha, Esq.
Direct Dial (202) 663-7915
Email: fosha@sughrue.com

December 26, 2000

BOX PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Re: Application of Masayuki TERAO, Akira SAKAI, Masakatsu TAKIZAWA, and Shuuji YAMAGUCHI
COMMUNICATION DEVICE, COMMUNICATION DEVICE SET, AUTHENTICATION METHOD AND METHOD OF WIRELESS-CONNECTING TERMINALS
Our Ref. Q62445

Dear Sir:

Attached hereto is the application identified above including 92 sheets of the specification, claims, 29 sheets of formal drawings, the executed Assignment and PTO 1595 form, and the executed Declaration and Power of Attorney. Also enclosed is an Information Disclosure Statement with Form PTO-1449 and references.

The Government filing fee is calculated as follows:

Total claims	34	- 20	=	14	x	$18.00	=	$252.00
Independent claims	11	- 3	=	8	x	$80.00	=	$640.00
Base Fee								$710.00
TOTAL FILING FEE								**$1602.00**
Recordation of Assignment								$40.00
TOTAL FEE								**$1642.00**

Checks for the statutory filing fee of $1602.00 and Assignment recordation fee of $40.00 are attached. You are also directed and authorized to charge or credit any difference or overpayment to Deposit Account No. 19-4880. The Commissioner is hereby authorized to charge any fees under 37 C.F.R. §§ 1.16 and 1.17 and any petitions for extension of time under 37 C.F.R. § 1.136 which may be required during the entire pendency of the application to Deposit Account No. 19-4880. A duplicate copy of this transmittal letter is attached.

Priority is claimed from December 27, 1999 based on Japanese Application No. 369706/99. The priority document is enclosed herewith.

Respectfully submitted,
SUGHRUE, MION, ZINN,
MACPEAK & SEAS, PLLC
Attorneys for Applicant

By: _____
J. Frank Osha
Registration No. 24,625

Terao et al #3
Filed 12/26/00
Q 62445
1 of 1

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年１２月２７日

出 願 番 号
Application Number: 平成１１年特許願第３６９７０６号

出 願 人
Applicant (s): 日本電気株式会社

２０００年 ９月 ８日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３０７２０９４

【書類名】　特許願

【整理番号】　62509030

【提出日】　平成11年12月27日

【あて先】　特許庁長官殿

【国際特許分類】　H04B　1/38

【発明者】

【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内

【氏名】　寺尾　正之

【発明者】

【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内

【氏名】　山口　修司

【発明者】

【住所又は居所】　東京都港区高輪二丁目２０番３６号　株式会社エヌイーシーデザイン内

【氏名】　坂井　晃

【発明者】

【住所又は居所】　東京都港区高輪二丁目２０番３６号　株式会社エヌイーシーデザイン内

【氏名】　滝澤　全克

【特許出願人】

【識別番号】　000004237

【氏名又は名称】　日本電気株式会社

【代理人】

【識別番号】　100088959

【弁理士】

【氏名又は名称】　境　廣巳

【手数料の表示】

【予納台帳番号】　009715

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9002136

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　通信装置、通信装置セット、認証方法および端末間ワイヤレス接続方法

【特許請求の範囲】

【請求項１】　端末装置のスロットに対して挿抜自在な通信装置であって、前記スロットに挿入されたときに端末装置から露出する部分が当該通信装置の種類に応じた色で色付けされている通信装置。

【請求項２】　所定の移動体通信サービスに適合する無線部を有し、移動体通信サービスの種類に応じた色で色付けされている請求項１記載の通信装置。

【請求項３】　特定のプロバイダーに接続するのに必要な情報が記憶された請求項２記載の通信装置。

【請求項４】　端末装置のスロットに対して挿抜自在でそれぞれ異なる移動体通信サービスに適合する無線部を有する複数の通信装置のセットであって、前記スロットに挿入されたときに端末装置から露出する部分が各通信装置毎にそれぞれ異なる色で色付けされている通信装置セット。

【請求項５】　端末装置のスロットに対して挿抜自在な通信装置と前記端末装置との間で認証を行う方法であって、

（ａ）通信装置に記憶されたＩＤと同じＩＤを記憶させたキーモジュールをスロットに挿入し、該キーモジュールに記憶されたＩＤを端末装置に登録するステップと、

（ｂ）端末装置とそのスロットに挿入された通信装置との間で、通信装置に記憶されたＩＤと端末装置に登録されたＩＤとが一致するか否かを照合するステップとを含む認証方法。

【請求項６】　端末装置のスロットに対して挿抜自在な通信装置と前記端末装置との間で認証を行う方法であって、

（ａ）通信装置に記憶されたＩＤおよび認証コードと同じＩＤおよび認証コードを記憶し且つ通信装置に記憶された逆暗号関数と対をなす暗号関数を記憶したキーモジュールをスロットに挿入し、該キーモジュールに記憶されたＩＤ、認証コード及び暗号関数を端末装置に登録するステップと、

（ｂ）通信装置がスロットに挿入されたとき、通信装置と端末装置との間で認証を行うステップとを含み、

前記ステップｂは、

（ｂ－１）通信装置に記憶されたＩＤと端末装置に登録されたＩＤとを照合するステップと、

（ｂ－２）ＩＤの照合が成功したときに、乱数を発生し、該乱数に認証コードを連結したものを暗号関数で暗号化したデータを端末装置から通信装置に送り、通信装置側では逆暗号関数によって認証コードと乱数を復元し、該復元した認証コードと記憶されている認証コードとを照合するステップと、

（ｂ－３）認証コードの照合が成功したときに、前記復元した乱数を逆暗号関数で暗号化したデータを通信装置から端末装置に送り、端末装置では暗号関数によって乱数を復元し、該復元した乱数と自ら生成した前記乱数とを照合するステップとを含む認証方法。

【請求項７】　端末装置と通信装置との間で認証が成立した後、通信装置がスロットから取り出されたとき、端末装置を利用者からの入力を一切受け付けないロック状態とする請求項５または６記載の認証方法。

【請求項８】　ロック状態の端末装置のスロットに通信装置が挿入されて端末装置と通信装置との間で認証が成立したとき、端末装置のロック状態を解除する請求項７記載の認証方法。

【請求項９】　端末装置間をワイヤレス接続する通信装置であって、伝送速度に応じた色で色付けされている請求項１記載の通信装置。

【請求項１０】　端末装置間をワイヤレス接続するために端末装置のスロットに対して挿抜自在な複数の通信装置のセットであって、各通信装置は、自通信装置の通信アドレス及び同セット中の他の通信装置の通信アドレスを記憶する、前記端末装置から読み取り可能なメモリを備えた通信装置セット。

【請求項１１】　各通信装置の前記メモリに、データ暗号化用の共通鍵を記憶してある請求項１０記載の通信装置セット。

【請求項１２】　各通信装置の前記メモリに、自通信装置の秘密鍵と同セット中の他の通信装置の公開鍵とを記憶してある請求項１０記載の通信装置セット

。

【請求項１３】　端末装置間をワイヤレス接続するために端末装置のスロットに対して挿抜自在な複数の通信装置のセットであって、各通信装置は、自通信装置の通信アドレス及びデータ暗号化用のセット固有の共通鍵を記憶する、前記端末装置から読み取り可能なメモリを備えた通信装置セット。

【請求項１４】　端末装置間をワイヤレス接続するために端末装置のスロットに対して挿抜自在な複数の通信装置のセットであって、各通信装置は、自通信装置の通信アドレス、データ暗号化用の公開鍵およびデータ復号化用の秘密鍵を記憶する、前記端末装置から読み取り可能なメモリを備えた通信装置セット。

【請求項１５】　端末装置のスロットに挿入されたときに端末装置から一部はみ出る部分に通信装置固有の番号が付記されており、通信装置の通信アドレスは上位アドレス部と下位アドレス部とから構成され、前記番号が下位アドレス部に設定されている請求項１０ないし１４の何れかに記載の通信装置セット。

【請求項１６】　端末装置間をワイヤレス接続するために端末装置のスロットに対して挿抜自在であり且つ自通信装置の通信アドレスを記憶するメモリを備えた複数の通信装置のセットを使って、複数の端末装置間をローカルにワイヤレス接続する方法であって、

（ａ）ワイヤレス接続する端末装置のそれぞれに通信装置を割り当てる段階、

（ｂ）各通信装置を割り当て先の端末装置以外の端末装置のスロットに挿入し、その通信装置のメモリに記憶された通信アドレスを挿入先の端末装置の送信先一覧テーブルに登録する段階、

（ｃ）各通信装置を割り当て先の端末装置のスロットに挿入する段階、

（ｄ）送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装置の通信アドレスを使用して、通信装置が挿入された端末装置間でデータを送受信する段階、

を含む端末間ワイヤレス接続方法。

【請求項１７】　各通信装置の前記メモリにセット固有の共通鍵を記憶し、送信データの暗号化および受信データの復号化に前記共通鍵を使用する請求項１６記載の端末間ワイヤレス接続方法。

【請求項１８】　端末装置間をワイヤレス接続するために端末装置のスロットに対して挿抜自在であり且つ自通信装置の通信アドレス、公開鍵および秘密鍵を記憶するメモリを備えた複数の通信装置のセットを使って、複数の端末装置間をローカルにワイヤレス接続する方法であって、

（ａ）ワイヤレス接続する端末装置のそれぞれに通信装置を割り当てる段階、

（ｂ）各通信装置を割り当て先の端末装置以外の端末装置のスロットに挿入し、その通信装置に記憶された通信アドレスおよび公開鍵を挿入先の端末装置の送信先一覧テーブルに登録する段階、

（ｃ）各通信装置を割り当て先の端末装置のスロットに挿入する段階、

（ｄ）送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装置の通信アドレスを使用し、送信データの暗号化に送信先通信装置の公開鍵を使用し、受信データの復号化に秘密鍵を使用して、通信装置が挿入された端末装置間でデータを送受信する段階、

を含む端末間ワイヤレス接続方法。

【請求項１９】　端末装置間をワイヤレス接続するために端末装置のスロットに対して挿抜自在であり且つ自通信装置の通信アドレスを記憶するメモリを備えた複数の通信装置のセットを使って、複数の端末装置間をローカルにワイヤレス接続する方法であって、

（ａ）ワイヤレス接続する端末装置のそれぞれに通信装置を割り当てる段階、

（ｂ）特定の端末装置のスロットに、他の端末装置に割り当てられた通信装置を順番に挿入し、その通信装置に記憶された通信アドレスを前記特定の端末装置の送信先一覧テーブルに登録する段階、

（ｃ）各通信装置を割り当て先の端末装置のスロットに挿入する段階、

（ｄ）前記特定の端末装置から他の端末装置に対して順番に、前記送信先一覧テーブルの内容を、今回の送信先通信装置の通信アドレス部分を前記特定の端末装置に挿入された通信装置に記憶された通信アドレスに置き換えて送信し、受信側各端末装置において受信した送信先一覧テーブルの内容を自装置の送信先一覧テーブルに設定する段階、

（ｅ）送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装

置の通信アドレスを使用して、通信装置が挿入された端末装置間でデータを送受信する段階、

を含む端末間ワイヤレス接続方法。

【請求項２０】　各通信装置の前記メモリにセット固有の共通鍵を記憶し、送信データの暗号化および受信データの復号化に前記共通鍵を使用する請求項１９記載の端末間ワイヤレス接続方法。

【請求項２１】　複数のスロットを有し且つスロット間のデータ中継機能を有する中継装置の１つのスロットに第１セットの通信装置を挿入し、他の１つのスロットに第２セットの通信装置を挿入し、第１セットの他の通信装置が挿入された端末装置と第２セットの他の通信装置が挿入された端末装置間を前記中継装置を介して通信可能とする請求項１６、１７または２０記載の端末間ワイヤレス接続方法。

【請求項２２】　端末装置間をワイヤレス接続するために端末装置のスロットに対して挿抜自在であり且つ自通信装置の通信アドレス、公開鍵および秘密鍵を記憶するメモリを備えた複数の通信装置のセットを使って、複数の端末装置間をローカルにワイヤレス接続する方法であって、

（ａ）ワイヤレス接続する端末装置のそれぞれに通信装置を割り当てる段階、

（ｂ）特定の端末装置のスロットに、他の端末装置に割り当てられた通信装置を順番に挿入し、その通信装置に記憶された通信アドレスおよび公開鍵を前記特定の端末装置の送信先一覧テーブルに登録する段階、

（ｃ）各通信装置を割り当て先の端末装置のスロットに挿入する段階、

（ｄ）前記特定の端末装置から他の端末装置に対して順番に、前記送信先一覧テーブルの内容を、今回の送信先通信装置の通信アドレスおよび公開鍵の部分を前記特定の端末装置に挿入された通信装置に記憶された通信アドレスおよび公開鍵に置き換えて送信し、受信側端末装置において受信した送信先一覧テーブルの内容を自装置の送信先一覧テーブルに設定する段階、

（ｅ）送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装置の通信アドレスを使用し、送信データの暗号化に送信先通信装置の公開鍵を使用し、受信データの復号化に秘密鍵を使用して、通信装置が挿入された端末装置

間でデータを送受信する段階、

を含む端末間ワイヤレス接続方法。

【請求項２３】　端末装置のスロットに挿入されたときに端末装置から一部はみ出る部分に通信装置固有の番号が付記されており、通信装置の通信アドレスは上位アドレス部と下位アドレス部とから構成され、前記番号が下位アドレス部に設定されている請求項１６ないし２２の何れかに記載の端末間ワイヤレス接続方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は端末装置に対して挿抜自在な通信装置に関し、また通信装置と端末装置との間の認証方法および通信装置を使って端末間をワイヤレス接続する方法に関する。

【０００２】

【従来の技術】

端末装置に対して挿抜自在な通信装置は、従来より各種のものが提案されている。例えば特開平８－１４９０３５号公報（以下、文献１と称す）では、情報端末とのインタフェース手段、アンテナ及び無線送受信回路を備え、情報端末のＰＣＭＣＩＡ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ　Ｍｅｍｏｒｙ　Ｃａｒｄ　Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ａｓｓｏｃｉａｔｉｏｎ）規格のスロットに挿入して使用するカード型無線通信装置が提案されている。また同文献１には、カード型無線通信装置に、ＧＳＭ（Ｇｌｏｂａｌ　Ｓｙｓｔｅｍ　ｆｏｒ　Ｍｏｂｉｌｅ　ｃｏｍｍｕｎｉｃａｔｉｏｎ）システムの個々の加入者に交付される認証モジュールを装着する部位を設け、認証モジュールを装着したカード型無線通信装置を情報端末に挿入したときにユーザから暗証番号を入力させ、この入力された暗証番号と認証モジュールに事前に設定された暗証番号とを照合することにより、他人による悪用を防止する技術も示されている。

【０００３】

ＰＣＭＣＩＡ規格のスロットなどに挿抜自在な通信装置としては、他に、特開

平８－３２１７９１号公報（以下、文献２と称す）に記載されたデータ通信用無線トランシーバーや、特開平１１－１５４８８６号公報（以下、文献３と称す）に記載された無線端末がある。

【０００４】

【発明が解決しようとする課題】

端末装置に対して挿抜自在な通信装置は、文献１～３に示されるように従来より各種のものが提案されているが、以下のような課題があった。

【０００５】

（１）一般に移動体通信サービスには、ＧＳＭシステム、ＣＤＭＡ（Ｃｏｄｅ Ｄｉｖｉｓｉｏｎ Ｍｕｌｔｉｐｌｅ Ａｃｃｅｓｓ）システム、ＰＤＣ（Ｐｅｒｓｏｎａｌ Ｄｅｇｉｔａｌ Ｃｅｌｌｕｌａｒ）システム、ＰＨＳ（Ｐｅｒｓｏｎａｌ Ｈａｎｄｙｐｈｏｎｅ Ｓｙｓｔｅｍ）システムなど各種のものがある。このため、種々の無線インフラに対応するためには、それぞれの移動体通信サービスに対応した通信装置を用意し、通信装置を差し替えて使用する必要がある。この場合に問題となるのは、現在使っている通信装置がどの移動体通信サービスに対応するものであるかを、ユーザが即座に認知できないことである。その理由は前記各文献１～３では、移動体通信サービスとして或る特定のものを前提としているため、通信装置の種類をユーザに認知させる構成となっていないからである。

【０００６】

（２）文献１に記載のカード型無線通信装置では、他人による悪用を防止するために暗証番号を利用しているが、そのためにユーザは、カード型無線通信装置を異なる端末装置に装着する都度、暗証番号を入力する必要があり、利便性が阻害される。

【０００７】

（３）従来のこの種の通信装置は、移動体通信サービスの使用を前提としている。このため、各個人が所有するＰＤＡ（Ｐａｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ａｓｓｉｓｔａｎｔ）、携帯電話、パーソナルコンピュータ（ＰＣ）などの各端末それぞれに通信装置を挿入し、通信装置間で通信することによって複数の端末間

をワイヤレス接続した場合、通信の都度、移動体通信サービスを利用しなければならない為に料金がかかり、また高速な通信が困難である。端末装置間をローカルに接続する技術に無線ＬＡＮシステムがあるが、規模が大きく且つ通信アドレスの設定に専門的な知識が必要になるため、一般家庭では手軽に利用できない。

【０００８】

本発明は以上のような事情に鑑みて提案されたものであり、その目的は、現在どのような通信装置を使用しているかをユーザが極めて容易に認知できるようにすることにある。

【０００９】

本発明の別の目的は、他人による通信装置の悪用を防止するために必要なユーザの作業量を削減することにある。

【００１０】

本発明の他の目的は、端末装置間を手軽にワイヤレス接続できるようにすることにある。

【００１１】

【課題を解決するための手段】

本発明の通信装置および通信装置セットは、端末装置のスロットに挿入されたときに端末装置から露出する部分が通信装置の種類に応じた色で色付けされている。これによって、どの移動体通信サービス用の通信装置であるかが、スロットに挿入された状態でも外部から即座に認識することができる。移動体通信サービスとしては、例えばＰＨＳシステム、ＰＤＣシステム、ＣＤＭＡシステムが考えられるが、それらに限定されない。また、通信装置を購入すればインターネットのプロバイダーへの接続が行えるようにするために、各通信装置は、特定のプロバイダーに接続するのに必要な情報を記憶するメモリを備えるよう構成されていても良い。

【００１２】

本発明の認証方法では、通信装置とは別にキーモジュールという部品を使う。キーモジュールは通信装置と同じ形をしており、端末装置のスロットに挿抜自在になっている。キーモジュールには、通信装置に記憶されたＩＤと同じＩＤが記

憶されており、通信装置を使用する予定の１つ或いは複数の端末装置のスロットに挿入して、ＩＤをキーモジュールから端末装置側に登録する。ＩＤを一旦登録したら、キーモジュールは持ち歩く必要はない。通信装置を端末装置のスロットに挿入して使用する際、端末装置と通信装置との間で、通信装置に記憶されたＩＤと端末装置に登録されたＩＤとが一致するか否かが調べられる。従来のようにユーザがパスワードを一々入力する必要がなく、ユーザの作業量が軽減される。また登録には必ずキーモジュールが必要であるため、パスワード入力より安全性が高い。ＩＤの一致のみ照合するのではなく、以下のように、より厳格に相互認証するようにしても良い。

【００１３】

キーモジュールに、通信装置に記憶されたＩＤおよび認証コードと同じＩＤおよび認証コードを記憶させておくと共に、通信装置に記憶された逆暗号関数と対をなす暗号関数を記憶させておき、それらを端末装置に登録し、通信装置がスロットに挿入されたとき、通信装置と端末装置との間で上記の各種のデータを用いて認証を行わせる。先ず、通信装置に記憶されたＩＤと端末装置に登録されたＩＤとを照合する。次に、ＩＤの照合が成功したときに、乱数を発生し、該乱数に認証コードを連結したものを暗号関数で暗号化したデータを端末装置から通信装置に送り、通信装置側では逆暗号関数によって認証コードと乱数を復元し、該復元した認証コードと記憶されている認証コードとを照合する。更に、認証コードの照合が成功したときに、前記復元した乱数を逆暗号関数で暗号化したデータを通信装置から端末装置に送り、端末装置では暗号関数によって乱数を復元し、該復元した乱数と自ら生成した前記乱数とを照合する。このように乱数を導入することにより、認証時に転送データが一意になるのを防止でき、悪意のある第三者に対して頑健な認証が実現できる。

【００１４】

端末装置と通信装置との間で認証が成立した後、通信装置がスロットから取り出されたとき、端末装置を利用者からの入力を一切受け付けないロック状態としても良い。こうすれば通信装置に鍵（キー）の機能を持たせることができる。なお、ロック状態の端末装置のスロットに通信装置が挿入されて端末装置と通信装

置との間で認証が成立したとき、端末装置のロック状態は解除される。

【００１５】

本発明の通信装置および通信装置セットは、また、端末装置間をワイヤレス接続する場合にも使用できる。その場合、伝送速度に応じた色で色付けされており、どの伝送速度のタイプであるかがスロットに挿入された状態でも外部から即座に認識することができるようになっている。

【００１６】

本発明の端末間ワイヤレス接続用の通信装置セットの一例は、各通信装置が自通信装置の通信アドレス及び同セット中の他の通信装置の通信アドレスを記憶するメモリを備えている。また、データ暗号化用に共通鍵を使用する場合、その共通鍵もメモリに記憶され、データ暗号化用に公開鍵、復号化用に秘密鍵を使用する場合、各通信装置のメモリに自通信装置の秘密鍵と同セット中の他の通信装置の公開鍵とが事前に記憶されている。各通信装置に同セット中の他の通信装置の通信アドレスが記憶されているため、或る端末装置のスロットにその端末装置に割り当てた通信装置を挿入すれば、その端末装置はその通信装置から通信アドレス情報を読み出すだけで、自通信装置の通信アドレスおよび通信相手となる他の通信装置の通信アドレスを認識できる。この為、通信アドレスを設定する作業からユーザは解放され、また暗号化したデータを送受信する際の鍵も事前に設定されているため、鍵の設定をユーザ自身が行う必要がなくなる。

【００１７】

本発明の端末間ワイヤレス接続用の通信装置セットの他の例は、各通信装置が同セットの他の通信装置の通信アドレスを記憶せず、自通信装置の通信アドレスだけを記憶している。このため、通信装置を使って複数の端末装置間をローカルにワイヤレス接続する場合、まず、ワイヤレス接続する端末装置のそれぞれに通信装置を割り当て、次に、各通信装置を割り当て先の端末装置以外の端末装置のスロットに挿入し、その通信装置のメモリに記憶された通信アドレスを挿入先の端末装置の送信先一覧テーブルに登録する。そして、各通信装置を割り当て先の端末装置のスロットに挿入し、以後、送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装置の通信アドレスを使用して、通信装置が挿入さ

れた端末装置間でデータを送受信する。

【００１８】

勿論、各通信装置の前記メモリにセット固有の共通鍵を記憶しておき、送信データの暗号化および受信データの復号化に前記共通鍵を使用するようにしても良い。また、セット固有の共通鍵を使うと異なるセットの通信装置間では通信が行えない。それを可能にするには、複数のスロットを有し且つスロット間のデータ中継機能を有する中継装置を使用すれば良い。つまり、中継装置の１つのスロットに第１セットの通信装置を挿入し、他の１つのスロットに第２セットの通信装置を挿入し、第１セットの他の通信装置が挿入された端末装置と第２セットの他の通信装置が挿入された端末装置間を前記中継装置を介して通信可能とする。

【００１９】

また、公開鍵、秘密鍵を使った暗号化方式によるデータ送信も可能である。この場合は、各通信装置のメモリに、自通信装置の通信アドレス、公開鍵および秘密鍵を記憶しておき、各通信装置を割り当て先の端末装置以外の端末装置のスロットに挿入し、その通信装置に記憶された通信アドレスおよび公開鍵を挿入先の端末装置の送信先一覧テーブルに登録する。そして、各通信装置を割り当て先の端末装置のスロットに挿入し、送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装置の通信アドレスを使用し、送信データの暗号化に送信先通信装置の公開鍵を使用し、受信データの復号化に秘密鍵を使用して、通信装置が挿入された端末装置間でデータを送受信する。

【００２０】

上記の方法は、２つ或いは３つといった少数の端末装置間をワイヤレス接続するのに好適である。しかし、ワイヤレス接続する端末装置の数が増えると、通信装置のスロットへの挿入回数が増え、ユーザの作業量が増える。以下のような方法によれば、端末装置数が増えてもユーザの作業量を少なく抑えることができる。先ず、特定の端末装置のスロットに、他の端末装置に割り当てられた通信装置を順番に挿入し、その通信装置に記憶された通信アドレスを前記特定の端末装置の送信先一覧テーブルに登録する。次に、各通信装置を割り当て先の端末装置のスロットに挿入し、前記特定の端末装置から他の端末装置に対して順番に、前記

送信先一覧テーブルの内容を、今回の送信先通信装置の通信アドレス部分を前記特定の端末装置に挿入された通信装置に記憶された通信アドレスに置き換えて送信し、受信側各端末装置において受信した送信先一覧テーブルの内容を自装置の送信先一覧テーブルに設定する。以後、送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装置の通信アドレスを使用して、通信装置が挿入された端末装置間でデータを送受信する。

【００２１】

勿論、各通信装置の前記メモリにセット固有の共通鍵を記憶しておき、送信データの暗号化および受信データの復号化に前記共通鍵を使用するようにしても良い。また、セット固有の共通鍵を使うと異なるセットの通信装置間では通信が行えないが、その場合には前述した中継装置を利用すれば良い。また、公開鍵、秘密鍵を使った暗号化方式によるデータ送信を行う場合は、各通信装置の前記メモリに自通信装置の通信アドレス、公開鍵および秘密鍵を記憶させておき、特定の端末装置のスロットに、他の端末装置に割り当てられた通信装置を順番に挿入し、その通信装置に記憶された通信アドレスおよび公開鍵を前記特定の端末装置の送信先一覧テーブルに登録する。次に、各通信装置を割り当て先の端末装置のスロットに挿入し、前記特定の端末装置から他の端末装置に対して順番に、前記送信先一覧テーブルの内容を、今回の送信先通信装置の通信アドレスおよび公開鍵の部分を前記特定の端末装置に挿入された通信装置に記憶された通信アドレスおよび公開鍵に置き換えて送信し、受信側端末装置において受信した送信先一覧テーブルの内容を自装置の送信先一覧テーブルに設定する。以後、送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装置の通信アドレスを使用し、送信データの暗号化に送信先通信装置の公開鍵を使用し、受信データの復号化に秘密鍵を使用して、通信装置が挿入された端末装置間でデータを送受信する。

【００２２】

また本発明の端末間ワイヤレス接続用の通信装置は、端末装置のスロットに挿入されたときに端末装置から一部はみ出る部分に通信装置固有の番号が付記されており、その通信装置の通信アドレスは上位アドレス部と下位アドレス部とから

構成され、前記番号が下位アドレス部に設定されている。これにより、ユーザは通信アドレスの下位アドレス部の値と通信装置に付記された番号とを見比べることによって、どの通信装置がどの通信アドレスに対応しているかを認識することができる。

【００２３】

【発明の実施の形態】

次に本発明の実施の形態の例について図面を参照して詳細に説明する。

【００２４】

図１を参照すると、本発明の一実施の形態は、携帯端末装置１ａ、ＰＤＡ１ｂ、ＰＣ（パーソナルコンピュータ）１ｃの３台の端末装置が、それぞれに設けられたスロット２ａ、２ｂ、２ｃに挿入された通信装置３ａ、３ｂ、３ｃによって相互にワイヤレス接続されている。通信装置３ａ～３ｃのそれぞれは、規格化された同一の外形形状を有し、また内部構造も全て同じになっている。通信装置３ａ～３ｃの構成例を図２に示す。

【００２５】

図２を参照すると、コネクタ３１は、装置筐体３０の一端側に設けられており、通信装置がスロット内に挿入されたときに通信装置側に設けられたソケットと物理的かつ電気的に結合する。アンテナ３２は、コネクタ３１と反対側の端部に設けられており、通信装置がスロットに装着された状態ではスロット外にはみ出る。アンテナ３２はスロットアンテナ等の小型アンテナで構成される。コネクタ３１とアンテナ３２との間には、インタフェイス３３、制御部３４、メモリ３５および無線部３６が設けられる。インタフェイス３３はコネクタ３１と信号線Ｌ１で接続されると共に信号線Ｌ２で制御部３４に接続され、制御部３４は信号線Ｌ３、Ｌ４でメモリ３５、無線部３６に接続され、無線部３６は信号線Ｌ５でアンテナ３２に接続される。また、コネクタ３１を通じて端末装置側から供給される電力が電源線３７を介して各部に供給される構成となっている。

【００２６】

メモリ３５は、ＲＯＭ等の不揮発性メモリで構成され、少なくとも自通信装置の通信アドレスを記憶している。メモリ３５に記憶された通信アドレスは、通信

装置の起動時に制御部３４で読み取られ、無線部３６に対して自通信装置の通信アドレスとして設定される。また、メモリ３５の記憶情報は、制御部３４、インタフェイス３３およびコネクタ３１を介して端末装置から読み取り可能になっている。

【００２７】

無線部３６は、無線周波数信号を生成し、伝送し、受信する機能を持つ。この無線部３６は、例えばＩＥＥＥ８０２．１として標準化されている無線ＬＡＮの規格に準拠した既存の無線ＬＡＮシステムにおける子機の無線部を流用して実現することができ、その場合、通信方式も直接拡散方式、周波数ホッピング方式など任意の方式を利用できる。また、ｂｌｕｅｔｏｏｔｈシステムで使われる無線部を流用することもできる。使用する周波数帯は２．４ＧＨｚ、４ＧＨｚ等、種々のタイプがある。また、媒体アクセス制御機能を持たせるようにしても良い。その場合、例えば、送信前にキャリアをセンスし、キャリアを検出したら送信を行わず、ランダム時間後に再送信を試みる分散制御型のＣＳＭＡ／ＣＡ（Ｃａｒｒｉｅｒ　Ｓｅｎｓｅ　Ｍｕｌｔｉｐｌｅ　Ａｃｃｅｓｓ　ｗｉｔｈ　Ｃｏｌｌｉｓｉｏｎ　Ａｖｏｉｄａｎｃｅ）が使用できる。

【００２８】

インタフェイス３３は、コネクタ３１と共に所定の電気的ないし機械的規格に適合するアダプタを構成する。規格としては、例えばＰＣＭＣＩＡ規格を採用することができるが、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）などの他の規格であっても良い。

【００２９】

制御部３４は、通信装置全体の制御を司る部分であり、例えばＭＰＵ及び制御用プログラムを記憶するＲＯＭ等で構成される。制御部３４は、無線部３６で受信された自通信装置宛のデータをインタフェイス３３及びコネクタ３１経由で端末装置に伝達する制御、端末装置側からコネクタ３１及びインタフェイス３３経由で伝達された送信データを無線部３６に伝達して送信させる制御といった送受信にかかる基本的な制御機能に加え、各種の付加的な制御機能を有する。

【００３０】

携帯端末装置１ａの構成例を図３に示す。図３を参照すると、携帯端末装置１ａは、装置筐体１００内に、キーパッド１０１、ＬＣＤ等の表示器１０２、アナログからデジタル及びその逆変換を行うＡ／Ｄ変換器１０３、これらと信号線Ｌ１１～Ｌ１３で接続された制御部１０４、Ａ／Ｄ変換器１０３に信号線Ｌ１４で接続されたマイク／スピーカ１０５、制御部１０４に信号線Ｌ１５で接続されたメモリ１０６、制御部１０４に信号線Ｌ１６で接続されたインタフェイス１０７及び各部に電力を供給する電源１０８を有し、またスロット２ａを備え、このスロット２ａ内に信号線Ｌ１７でインタフェイス１０７と接続されたソケット１０９が設けられている。

【００３１】

ソケット１０９とインタフェイス１０７は、図２に示す通信装置３ａ～３ｃ側のアダプタ（３１、３３）に電気的ないし機械的に適合するアダプタを構成する。Ａ／Ｄ変換器１０３は、マイクからのアナログ音声信号をデジタル音声信号へ変換し、制御部１０４からスピーカへ出力される音声信号をデジタル信号からアナログ信号へ変換する。制御部１０４は、一般の携帯電話が有する送受話制御機能に加えて、各種の付加的な機能を有し、例えばＭＰＵ及び制御プログラムを記憶するＲＯＭで構成される。メモリ１０６は、例えばＲＡＭで構成され、各種のデータを記憶するために利用される。

【００３２】

ＰＤＡ１ｂの構成例を図４に示す。図４を参照すると、ＰＤＡ１ｂは、装置筐体１１０内に、ＭＰＵ１１１とそのバス１１２に接続されたＲＯＭ１１３、ＲＡＭ１１４、キーボードコントローラ１１５、表示コントローラ１１６、タブレットコントローラ１１７およびインタフェイス１１８と、キーボードコントローラ１１５に信号線Ｌ３１で接続されたキーボード１１９と、表示コントローラ１１６に信号線Ｌ３２で接続されたＬＣＤ等の表示器１２０と、タブレットコントローラ１１７に信号線Ｌ３３で接続されたタブレット１２１と、各部に電力を供給する電源１２２とを有し、またスロット２ｂを備え、このスロット２ｂ内に信号線Ｌ３４でインタフェイス１１８と接続されたソケット１２３が設けられている。

【００３３】

ソケット１２３とインタフェイス１１８は、通信装置３ａから３ｃ側のアダプタ（３１、３３）に電気的ないし機械的に適合するアダプタを構成する。タブレット１２１は表示器１２０の表示面を覆うように配置されており、表示器１２０及びそれらのコントローラ１１６、１１７と共にペン入力機能付き表示装置を構成する。ＭＰＵ１１１は、ＰＤＡ１ｂ全体の制御を司る制御部を構成し、ＲＯＭ１１３はＭＰＵ１１１で実行する各種のプログラムを記憶する。ＲＡＭ１１４は各種のデータを記憶するために利用される。

【００３４】

ＰＣ１ｃは、ＰＤＡ１ｂと基本的に同じ構成を有する。但し、ペン入力方式でないＰＣではタブレット１２１およびタブレットコントローラ１１７は省略される。また一般にマウス入力が可能であり、電源も通常は商用電源が利用される。

【００３５】

次に、端末装置間をワイヤレス接続する実施例について説明する。

【００３６】

【実施例１】

通信装置は複数本を１セットとしてユーザに販売される。含まれる通信装置の数の違いによって、また伝送速度の違いによって、様々なセットが存在する。例えば或るセットは、伝送速度２Ｍｂｐｓの２個の通信装置から構成され、他のセットは伝送速度４Ｍｂｐｓの１０個の通信装置から構成される。各セット中の通信装置は、スロットに挿入されたときにスロット外にはみ出る部分に伝送速度に応じた色が塗られており、色によって通信装置の伝送速度が認識できるようになっている。例えば、２Ｍｂｐｓは黄色、４Ｍｂｐｓはオレンジ、１０Ｍｂｐｓは赤、１６Ｍｂｐｓは青、３２Ｍｐｂｓは緑である。なお、通信装置はスロット外にはみ出る必要は必ずしもなく、露出していれば良い。また、各セット中の通信装置には１から始まる連続番号が付記されている。価格は伝送速度が早くなれば高くなり、またセットに含まれる通信装置の個数が増えるほど高くなる。ユーザは、伝送速度と本数を決め、該当するセットを購入する。通信装置の個数は、ワイヤレス接続したい端末装置の総台数以上必要である。

【００３７】

図５に、ユーザが購入した１セット分の通信装置の外観の概略を示す。この例のセットは３個組みのセットであり、通信装置３ａには「１」、通信装置３ｂには「２」、通信装置３ｃには「３」がそれぞれ印刷ないし刻字されている。伝送速度を示す色は、１～３の数字が色付け数字とされるか、または背景が着色される。後者の場合、端部全面を着色しても良く、一部を着色しても良い。

【００３８】

本実施例の場合、同じセットの各通信装置３ａ～３ｂのメモリ３５には、図５に付記するように、自通信装置の通信アドレス、他通信装置の通信アドレス、データ送信時に使う暗号化用の共通鍵が予め記憶されている。通信アドレスは、複数ビットで構成される上位アドレス部と、数ビットで構成される下位アドレス部とから成り、上位アドレス部には当該セット固有のアドレスが設定され、下位アドレス部にはその通信装置に付記された連続番号の数値が設定されている。

【００３９】

図５に示した３個の通信装置３ａ～３ｃを使って、図１に示した３台の端末装置１ａ～１ｃをワイヤレス接続する場合、各端末装置１ａ～１ｃにそれぞれ１個の通信装置３ａ～３ｃを割り当て、それぞれ登録作業を行う。以下、端末装置１ａに通信装置３ａを、端末装置１ｂに通信装置３ｂを、端末装置１ｃに通信装置３ｃをそれぞれ割り当てたものとして、本実施例における登録作業について説明する。

【００４０】

携帯端末装置１ａのキーパッド１０１を操作して、ワイヤレス接続用の通信装置の登録処理を起動すると、制御部１０４は、図６に示す処理を開始する。先ず、表示器１０２に「スロットに通信装置を挿入して下さい」といったメッセージを表示する（Ｓ１）。これに応じてユーザがスロット２ａに通信装置３ａを挿入すると、携帯端末装置１ａに内蔵の電源１０８からソケット１０９を通じて通信装置３ａに電力が供給されて通信装置３ａが動作可能状態になる。次に、制御部１０４は、インタフェイス１０７、ソケット１０９および通信装置３ａのコネクタ３１、インタフェイス３３および制御部３４を通じて、メモリ３５に記憶され

た自通信装置３ａの通信アドレス、他通信装置３ｂ、３ｃの通信アドレスおよび共通鍵Ｋを読み込む（Ｓ２）。そして、自通信装置情報テーブルを生成し（Ｓ３）、送信先一覧テーブルを生成し（Ｓ４）、送信先選択画面を生成し（Ｓ５）、登録完了メッセージを表示器１０２に表示し（Ｓ６）、処理を終了する。それぞれ生成された自通信装置情報テーブル、送信先一覧テーブルおよび送信先選択画面は、メモリ１０６に保存される。

【００４１】

ステップＳ３で生成される自通信装置情報テーブルの内容例を図７（ａ）に示す。自通信装置情報テーブル１３０は、通信装置番号、通信アドレス、鍵の項目から構成される。通信アドレスには、自通信装置３ａの通信アドレスが設定され、通信装置番号には、自通信装置３ａの通信アドレスの下位アドレス部で示される数値、つまり通信装置３ａに付記された番号１が設定される。鍵には、共通鍵Ｋが設定される。

【００４２】

ステップＳ４で生成される送信先一覧テーブルの内容例を図７（ｂ）に示す。送信先一覧テーブル１３１は、他通信装置３ｂ、３ｃ毎のエントリで構成され、各エントリは通信装置番号、通信アドレス、鍵の項目を含む。通信アドレスには、他通信装置３ｂ、３ｃの通信アドレスが設定される。通信装置番号には、他通信装置３ｂ、３ｃの通信アドレスの下位アドレス部で示される数値、つまり他通信装置３ｂ、３ｃに付記された番号２、３が設定される。鍵には、共通鍵Ｋが設定される。

【００４３】

ステップＳ５で生成される送信先選択画面は、実際の送信時に送信先をユーザに選択させる際に使用する画面であり、その内容例を図７（ｃ）に示す。同図に示されるように送信先選択画面は、送信先一覧テーブル１３１に設定された通信装置番号２、３をユーザに提示し、その何れかを選択させる画面である。

【００４４】

図６に示したような登録作業を支援する機能は、ＰＤＡ１ｂおよびＰＣ１ｃのＭＰＵ１１１によっても提供されており、ユーザはＰＤＡ１ｂおよびＰＣ１ｃに

対し通信装置３ｂ、３ｃを使用して携帯端末装置１ａと同様な作業を繰り返す。これによって、ＰＤＡ１ｂおよびＰＣ１ｃのＲＡＭ１１４に、図７と同様な自通信装置情報テーブル、送信先一覧テーブルおよび送信先選択画面が生成される。但し、通信装置３ａと通信装置３ｂ、通信装置３ｃとでは、自通信装置、他通信装置が異なるので内容は同じでない。

【００４５】

以上のような登録作業が完了すると、携帯端末装置１ａ、ＰＤＡ１ｂ、ＰＣ１ｃ間で相互にデータのワイヤレス送受信が可能となる。例えば携帯端末装置１ａのメモリ１０６に記憶された或る種のファイル（例えば電話帳ファイル）を送信対象ファイルに選択し、図７（ｃ）に示した送信先選択画面で例えば２番を選択して、キーパッド１０１の操作で送信開始を指示すると、制御部１０４は、ワイヤレス送信制御を開始する。先ず、送信対象ファイルをメモリ１０６から読み出し、自通信装置情報テーブル１３０に記憶されている共通鍵Ｋで暗号化する。そして、例えば図８に示すようなヘッダ１４０、送信先アドレス１４１、送信元アドレス１４２、送信データ１４３及びそのパリティビット等のチェックビット１４４から構成されるフォーマットの送信データを生成し、インタフェイス１０７を通じて通信装置３ａに送り込む。ここで、送信先アドレス１４１は、送信先選択画面にてユーザが選択した番号に対応して送信先一覧テーブル１３１に記憶されている通信アドレスであり、送信元アドレス１４２は自通信装置情報テーブル１３０に記憶されている通信アドレスである。また、送信データ１４３は共通鍵Ｋで暗号化されている。通信装置３ａの制御部３４は、端末装置１ａ側からの送信データをインタフェイス３３を介して受信すると、それを無線部３６に送り込み、無線部３６は無線周波数信号に変換し、アンテナ３２から送信する。

【００４６】

各端末装置１ａ～１ｂに挿入された各通信装置３ａ～３ｃにおける無線部３６は、アンテナ３２で受信されるデータの送信先アドレス１４１が自通信装置の通信アドレスと一致した場合、当該送信データを取り込み、制御部３４に伝達する。制御部３４は、この送信データをインタフェイス３３を通じて端末装置側に送り込む。例えば、送信先アドレス１４１に番号２のＰＤＡ１ｂに挿入された通信

装置１ｂの通信アドレスが設定されている場合、通信装置３ａから送信されたデータは通信装置３ｂで受信され、ＰＤＡ１ｂに送り込まれる。ＰＤＡ１ｂのＭＰＵ１１１は、データをインタフェイス１１８を通じて受け取り、チェックビット１４４によるチェックを行った後、誤りがなければ送信データ１４３を自通信情報テーブルに設定された共通鍵で復号化する。復号化されたデータは例えばその送信元アドレスと共にＲＡＭ１１４の受信エリアに格納され、その後、ＰＤＡ１ｂのユーザにデータの受信を知らせるメッセージが表示器１２０に表示される。

【００４７】

以上は携帯端末装置１ａからＰＤＡ１ｂへのワイヤレス送信であるが、ＰＤＡ１ｂから携帯端末装置１ａやＰＣ１ｃへのワイヤレス送信等、任意の装置間でも同様なワイヤレス送信が可能である。

【００４８】

【実施例２】

本実施例では、暗号化用の鍵として、通信装置固有の公開鍵を使用し、その復号に秘密鍵を使用する点で実施例１と相違し、その他の点は実施例１と同じである。図９に、ユーザが購入した１セット分の通信装置の外観の概略を示す。この例のセットは３個組みのセットであり、各通信装置３ａ～３ｂのメモリ３５には、自通信装置の通信アドレス、他通信装置の通信アドレス、自通信装置の秘密鍵、他通信装置の公開鍵が予め記憶されている。図９に示した３個の通信装置３ａ～３ｃを使って、図１に示した３台の端末装置１ａ～１ｃをワイヤレス接続する場合、実施例１と同様な登録作業を行う。このとき図６のステップＳ２では、自通信装置および他通信装置の通信アドレスと、自通信装置の秘密鍵と、他通信装置の公開鍵とが読み込まれ、図７の自通信装置情報テーブル１３０の鍵の項目に自通信装置の秘密鍵が設定され、送信先一覧テーブル１３１の鍵の項目には他通信装置の公開鍵が設定される。送信元の端末装置では、送信先端末装置の通信装置の公開鍵を使ってデータを暗号化して送信し、受信側の端末装置では自通信装置の秘密鍵を使って復号化する。

【００４９】

【実施例３】

本実施例では、暗号化用の鍵として、通信装置固有の公開鍵を使用し、その復号に秘密鍵を使用する点、それぞれの通信装置は自通信装置の通信アドレス、公開鍵および秘密鍵を記憶し、他通信装置の通信アドレス、公開鍵および秘密鍵は記憶していない点で実施例１と相違し、その他の点は実施例１と同じである。図１０に、ユーザが購入した１セット分の通信装置の外観の概略を示す。この例のセットは３個組みのセットであり、各通信装置３ａ～３ｂのメモリ３５には、自通信装置の通信アドレス、自通信装置の秘密鍵および公開鍵が予め記憶されている。

【００５０】

図１０に示した３個の通信装置３ａ～３ｃを使って、図１に示した３台の端末装置１ａ～１ｃをワイヤレス接続する場合、各端末装置１ａ～１ｃにそれぞれ１個の通信装置３ａ～３ｃを割り当て、所定の登録作業を行う。以下、端末装置１ａに通信装置３ａを、端末装置１ｂに通信装置３ｂを、端末装置１ｃに通信装置３ｃをそれぞれ割り当てたものとして、本実施例における登録作業について説明する。

【００５１】

先ず、各端末装置１ａ～１ｃに自通信装置３ａ～３ｃの通信アドレス、秘密鍵及び公開鍵を登録する作業を説明する。

【００５２】

携帯端末装置１ａのキーパッド１０１を操作して、ワイヤレス接続用の自通信装置の登録処理を起動すると、制御部１０４は、図１１に示す処理を開始する。先ず、表示器１０２に「スロットに自通信装置を挿入して下さい」といったメッセージを表示する（Ｓ１１）。これに応じてユーザがスロット２ａに自通信装置３ａを挿入すると、携帯端末装置１ａに内蔵の電源１０８からソケット１０９を通じて通信装置３ａに電力が供給されて通信装置３ａが動作可能状態になる。次に、制御部１０４は、インタフェイス１０７、ソケット１０９および通信装置３ａのコネクタ３１、インタフェイス３３および制御部３４を通じて、メモリ３５に記憶された自通信装置３ａの通信アドレス、自通信装置３ａの秘密鍵および公開鍵を読み込む（Ｓ１２）。そして、自通信装置情報テーブルを生成し（Ｓ１３

）、登録完了メッセージを表示器１０２に表示し（Ｓ１４）、処理を終了する。生成された自通信装置情報テーブルは、メモリ１０６に保存される。

【００５３】

ステップＳ１３で生成される自通信装置情報テーブルの内容例を図１２（ａ）に示す。自通信装置情報テーブル１４０は、通信装置番号、通信アドレス、鍵の項目から構成される。通信アドレスには、自通信装置３ａの通信アドレスが設定され、通信装置番号には、自通信装置３ａの通信アドレスの下位アドレス部で示される数値、つまり通信装置３ａに付記された番号１が設定される。鍵には、自通信装置３ａの秘密鍵および公開鍵が設定される。

【００５４】

図１１に示したような自通信装置に関する登録作業を支援する機能は、ＰＤＡ１ｂおよびＰＣ１ｃのＭＰＵ１１１によっても提供されており、ユーザはＰＤＡ１ｂおよびＰＣ１ｃに対し通信装置３ｂ、３ｃを使って携帯端末装置１ａと同様な作業を繰り返す。これによって、ＰＤＡ１ｂおよびＰＣ１ｃのＲＡＭ１１４に、図７（ａ）と同様な自通信装置情報テーブルが保存される。但し、通信装置３ａと通信装置３ｂ、通信装置３ｃとでは、通信アドレス、秘密鍵、公開鍵が異なるので内容は同じでない。

【００５５】

次に、各端末装置１ａ～１ｃに対して、他の端末装置に割り当てた通信装置３ａ～３ｃの通信アドレスおよび公開鍵を登録する作業について説明する。

【００５６】

携帯端末装置１ａのキーパッド１０１を操作して、ワイヤレス接続用の他通信装置の登録処理を起動すると、制御部１０４は、図１３に示す処理を開始する。先ず、表示器１０２に「スロットに他通信装置を挿入して下さい」といったメッセージを表示する（Ｓ３１）。これに応じてユーザがスロット２ａに例えば通信装置３ｂを挿入すると、携帯端末装置１ａに内蔵の電源１０８によって通信装置３ｂが動作可能状態になる。次に、制御部１０４は、インタフェイス１０７、ソケット１０９および通信装置３ａのコネクタ３１、インタフェイス３３および制御部３４を通じて、メモリ３５に記憶された通信装置３ｂの通信アドレス、通信

装置３ａの公開鍵を読み込み、メモリ１０６に一時的に保持する（Ｓ３２）。次に制御部１０４は他通信装置が他にあるか否かを表示器１０２にメッセージを表示してユーザに問い合わせ、他の通信装置がある場合（Ｓ３３でＮＯ）、ステップＳ３１に戻って上述した処理を繰り返す。今の場合、通信装置３ｃが残っているので、ユーザが通信装置３ｂに代えて通信装置３ｃをスロット２ａに挿入すると、通信装置３ｃの通信アドレス、公開鍵が読み込まれ、メモリ１０６に一次的に保持される。

【００５７】

他通信装置３ｂ、３ｃの通信アドレス及び公開鍵を携帯端末装置１ａに登録し終え、ユーザが他通信装置の終了をキーパッド１０１から入力すると（ステップＳ３３でＹＥＳ）、制御部１０４は、送信先一覧テーブルを生成し（Ｓ３４）、送信先選択画面を生成し（Ｓ３５）、登録完了メッセージを表示器１０２に表示し（Ｓ３６）、処理を終了する。生成された送信先一覧テーブル、送信先選択画面は、メモリ１０６に保存される。

【００５８】

ステップＳ３４で生成される送信先一覧テーブルの内容例を図１２（ｂ）に示す。送信先一覧テーブル１４１は、他通信装置３ｂ、３ｃ毎のエントリで構成され、各エントリは通信装置番号、通信アドレス、鍵の項目を含む。通信アドレスには、他通信装置３ｂ、３ｃの通信アドレスが設定される。通信装置番号には、他通信装置３ｂ、３ｃの通信アドレスの下位アドレス部で示される数値、つまり他通信装置３ｂ、３ｃに付記された番号２、３が設定される。鍵には、通信装置３ｂ、３ｃの公開鍵が設定される。

【００５９】

ステップＳ３５で生成される送信先選択画面は、図１２（ｃ）に示すように、図７（ｃ）に示したものと同じである。

【００６０】

図１３に示したような他通信装置の登録作業を支援する機能は、ＰＤＡ１ｂおよびＰＣ１ｃのＭＰＵ１１１によっても提供されており、ユーザはＰＤＡ１ｂおよびＰＣ１ｃに対して携帯端末装置１ａと同様な作業を繰り返す。これによって

、ＰＤＡ１ｂおよびＰＣ１ｃのＲＡＭ１１４に、図１２と同様な送信先一覧テーブルおよび送信先選択画面が保存される。但し、ＰＤＡ１ｂには通信装置３ａと通信装置３ｃの通信アドレス及び公開鍵が登録され、ＰＣ１ｃには通信装置３ａと通信装置３ｂの通信アドレス及び公開鍵が登録されるので、内容は同じでない。

【００６１】

以上のような登録作業が完了すると、実施例１と同様に携帯端末装置１ａ、ＰＤＡ１ｂ、ＰＣ１ｃ間で相互にデータのワイヤレス送受信が可能となる。

【００６２】

本実施例では、携帯端末装置１ａ、ＰＤＡ１ｂ、ＰＣ１ｃを相互にワイヤレス接続したが、そのような構成に限定されない。例えば、携帯端末装置１ａとＰＤＡ１ｂとの間の接続が不要であれば、携帯端末装置１ａには他通信装置としてＰＣ１ｃの通信装置３ｃのみを登録し、ＰＤＡ１ｂには他通信装置として携帯端末装置１ａの通信装置３ａのみを登録すれば良い。

【００６３】

【実施例４】

本実施例では、ワイヤレス接続しようとする複数の端末装置のうちの何れか１つを情報配信サーバとし、サーバから他の全ての端末装置に対して送信先一覧テーブルを配信するようにした点で実施例３と相違し、その他の点は実施例１と同じである。本実施例の場合、図１０に示した３個の通信装置３ａ～３ｃをそれぞれ割り当て先の端末装置１ａ、１ｂ、１ｃのスロットに挿入して、各端末装置１ａ～１ｃの自通信装置情報テーブルに図１２（ａ）に示したような自通信装置３ａ～３ｃの通信アドレス、秘密鍵及び公開鍵を登録した後、例えば端末装置１ａを情報配信サーバとして、各端末装置１ａ～１ｃに、他の端末装置に割り当てた通信装置３ａ～３ｃの通信アドレスおよび公開鍵を登録する作業を行う。

【００６４】

携帯端末装置１ａのキーパッド１０１を操作して、ワイヤレス接続用の他通信装置の登録処理を起動すると、制御部１０４は、図１４に示す処理を開始する。ステップＳ３１からステップＳ３５までは実施例３と同じ処理であり、図１２（

ｂ）、（ｃ）に示したような送信先一覧テーブル１４１および送信先選択画面１４２が端末装置１ａに生成される。続いて制御部１０４は、各端末装置にそれに割り当てた通信装置を挿入するよう促すメッセージを表示器１０２に表示する（Ｓ３７）。ユーザは、このメッセージに従ってスロットへの通信装置の挿入作業を行う。

【００６５】

次に制御部１０４は、送信先一覧テーブル１４１から１つの他通信装置、例えば通信装置３ｂを選択し（Ｓ３８）、送信先一覧テーブル１４１中の当該選択した通信装置３ｂにかかる通信装置番号、通信アドレス、公開鍵を、自通信装置情報テーブル１４０中の自通信装置３ａにかかる通信装置番号、通信アドレス、公開鍵で置き換えた配信用の送信先一覧テーブルを生成する（Ｓ４０）。そして、この送信先一覧テーブルを、自装置１ａのスロット２ａに挿入された通信装置３ａを使って、前記選択した通信装置３ｂがスロット２ａに挿入されたＰＤＡ１ｂに送信する（Ｓ４１）。この送信では、送信先アドレスに通信装置３ｂの通信アドレスを設定する。また、送信先一覧テーブルは通信装置３ｂの公開鍵で暗号化しておく。

【００６６】

ＰＤＡ１ｂのスロット２ｂに挿入された通信装置３ｂは、上記の配信データを受信すると、それをＰＤＡ１ｂに伝達し、ＰＤＡ１ｂのＭＰＵ１１１は、自通信装置３ｂの秘密鍵で復号化し、得られた送信先一覧テーブルをＲＡＭ１１４に記憶する。また、送信先一覧テーブルに登録された通信装置番号に基づき送信先選択画面を生成し、ＲＡＭ１１４に記憶する。

【００６７】

携帯端末装置１ａの制御部１０４は、ＰＤＡ１ｂに対する配信を終えると、次に通信装置３ｃを選択し（Ｓ３８）、送信先一覧テーブル１４１中の当該選択した通信装置３ｃにかかる通信装置番号、通信アドレス、公開鍵を、自通信装置情報テーブル１４０中の自通信装置３ａにかかる通信装置番号、通信アドレス、公開鍵で置き換えた配信用の送信先一覧テーブルを生成し（Ｓ４０）、ＰＣ１ｃに送信する（Ｓ４１）。ＰＣ１ｃのスロット２ｃに挿入された通信装置３ｃは、上

記の配信データを受信すると、それをＰＣ１ｃに伝達し、ＰＣ１ｃのＭＰＵ１１１は、自通信装置３ｃの秘密鍵で復号化し、得られた送信先一覧テーブルをＲＡＭ１１４に記憶する。また、送信先一覧テーブルに登録された通信装置番号に基づき送信先選択画面を生成し、ＲＡＭ１１４に記憶する。

【００６８】

携帯端末装置１ａの制御部１０４は、送信先一覧テーブル１４１に未処理の通信装置が残っていないことを確認し（Ｓ３９でＹＥＳ）、登録完了メッセージを表示して（Ｓ３６）、処理を終える。

【００６９】

【実施例５】

本実施例は、実施例３と実施例４とを組み合わせたものである。つまり、実施例３の構成によってワイヤレス接続された複数の端末装置の何れかを情報配信サーバに設定して、新たな通信相手の登録を実施例４の構成によって実現するものである。例えば図１５に示すように、無線でワイヤレス接続された通信装置Ａ１、Ａ２、Ａ０と、同じく無線でワイヤレス接続された通信装置Ｃ０、Ｃ１と、同じく無線でワイヤレス接続された通信装置Ｅ０、Ｅ１との３つのグループがある状況の下で、新たな通信装置Ｂ０、Ｄ０を導入し、通信装置Ａ０、Ｂ０、Ｃ０、Ｄ０、Ｅ０を相互にワイヤレス接続する場合について、本実施例の動作を説明する。なお、説明の便宜上、通信装置Ａ０は携帯端末装置１ａに挿入された通信装置３ａとする。

【００７０】

先ず、実施例４と同様にして、新たな通信装置Ｂ０、Ｄ０の通信アドレス、秘密鍵及び公開鍵を、それらが割り当てられた端末装置に登録する。

【００７１】

次に、携帯端末装置１ａのキーパッド１０１を操作して、ワイヤレス接続用の他通信装置の追加処理を起動すると、制御部１０４は、図１６に示す処理を開始する。先ず、表示器１０２に「スロットに追加する他通信装置を挿入して下さい」といったメッセージを表示する（Ｓ５１）。これに応じてユーザがスロット２ａに例えば通信装置Ｂ０を挿入すると、携帯端末装置１ａに内蔵の電源１０８に

よって通信装置Ｂ０が動作可能状態になる。次に、制御部１０４は、インタフェイス１０７、ソケット１０９および通信装置Ｂ０のコネクタ３１、インタフェイス３３および制御部３４を通じて、メモリ３５に記憶された通信装置Ｂ０の通信アドレス、通信装置Ｂ０の公開鍵を読み込み、メモリ１０６に一時的に保持する（Ｓ５２）。次に制御部１０４は他通信装置が他にあるか否かを表示器１０２にメッセージを表示してユーザに問い合わせ、他の通信装置がある場合、ステップＳ５１に戻って上述した処理を繰り返す。今の場合、通信装置Ｄ０、Ｃ０、Ｅ０が残っているので、ユーザが通信装置Ｂ０に代えて順次にそれらの通信装置をスロット２ａに挿入すると、各通信装置の通信アドレス、公開鍵が読み込まれ、メモリ１０６に一次的に保持される。

【００７２】

通信装置Ｂ０、Ｄ０、Ｃ０、Ｅ０の通信アドレス及び公開鍵を携帯端末装置１ａに登録し終え、ユーザが追加他通信装置の終了をキーパッド１０１から入力すると（Ｓ５３でＹＥＳ）、制御部１０４は、サーバ用送信先一覧テーブルを生成し（Ｓ５４）、既にメモリ１０６に生成済の送信先一覧テーブルおよび送信先選択画面を更新する（Ｓ５５、Ｓ５６）。ここで、サーバ用送信先一覧テーブルは、追加された通信装置Ｂ０、Ｄ０、Ｃ０、Ｅ０の通信装置番号、通信アドレス、公開鍵を設定したテーブルである。また、送信先一覧テーブルおよび送信先選択画面には、サーバ用送信先一覧テーブルに設定された通信装置の情報が追加される。

【００７３】

続いて制御部１０４は、各端末装置にそれに割り当てた通信装置を挿入するよう促すメッセージを表示器１０２に表示する（Ｓ５７）。ユーザは、このメッセージに従ってスロットへの通信装置の挿入作業を行う。

【００７４】

次に制御部１０４は、サーバ用送信先一覧テーブルから１つの他通信装置、例えば通信装置Ｂ０を選択し（Ｓ５８）、サーバ用送信先一覧テーブル中の当該選択した通信装置Ｂ０にかかる通信装置番号、通信アドレス、公開鍵を、自通信装置情報テーブル中の自通信装置Ａ０にかかる通信装置番号、通信アドレス、公開

鍵で置き換えた配信用の送信先一覧テーブルを生成する（Ｓ６０）。そして、この送信先一覧テーブルを、自装置のスロット２ａに挿入された通信装置Ａ０を使って、前記選択した通信装置Ｂ０がスロットに挿入された端末装置に送信する（Ｓ６１）。この送信では、送信先アドレスに通信装置Ｂ０の通信アドレスを設定する。また、送信先一覧テーブルは通信装置Ｂ０の公開鍵で暗号化しておく。

【００７５】

通信装置Ｂ０は、上記の配信データを受信すると、それをスロットを通じて端末装置に伝達し、端末装置の制御部は、自通信装置Ｂ０の秘密鍵で復号化し、得られた送信先一覧テーブルをメモリに記憶する。また、送信先一覧テーブルに登録された通信装置番号に基づき送信先選択画面を生成し、メモリに記憶する。

【００７６】

携帯端末装置１ａの制御部１０４は、通信装置Ｂ０に対する配信を終えると、同様の処理を通信装置Ｄ０、通信装置Ｃ０、通信装置Ｅ０に対して行う。通信装置Ｄ０側では通信装置Ｂ０と同じ動作が行われ、また通信装置Ｃ０、Ｅ０では、送信先一覧テーブルおよび送信先選択画面が既に作成されているので、送られてきた情報でそれらを更新する。制御部１０４は、通信装置Ｂ０、Ｄ０、Ｃ０、Ｅ０に対する配信を終えると、登録完了メッセージを表示し（Ｓ６２）、処理を終える。

【００７７】

以上のような登録作業が完了することにより、通信装置Ａ０、Ｂ０、Ｃ０、Ｄ０、Ｅ０相互の通信が可能になる。但し、通信装置Ｂ０から通信装置Ａ１、Ａ２、Ｃ１、Ｅ１、通信装置Ｃ０から通信装置Ａ１、Ａ２、Ｅ１、通信装置Ｄ０から通信装置Ａ１、Ａ２、Ｃ１、Ｅ１、通信装置Ｅ０から通信装置Ａ１、Ａ２、Ｃ１へは、それぞれ通信できない。

【００７８】

【実施例６】

本実施例では、中継装置を使って異なるセットの通信装置間での通信を実現する。その構成例を図１７に示す。端末装置１５０～１５２はそれぞれのスロットに挿入された通信装置Ａ０～Ａ３によって相互にワイヤレス接続されている。ま

た、端末装置１６０～１６２はそれぞれのスロットに挿入された通信装置Ｆ０～Ｆ３によって相互にワイヤレス接続されている。ここで、通信装置Ａ０～Ａ３は同じセットの通信装置であり、共通鍵としてＫ１を使用する。他方、通信装置Ｆ０～Ｆ３も同じセットの通信装置であり、共通鍵としてＫ２を使用する。共通鍵が異なるので、端末装置１５０と端末装置１６０とは直接に通信することはできない。中継装置１７０は、このような異なるセット間の通信を中継する装置であり、２つのスロット１７１、１７２を持ち、またソケット１７３、インタフェイス１７４、制御部１７５、メモリ１７６を備えている。

【００７９】

先ず、実施例３で説明した方法によって、スロット１７１に通信装置Ａ０と同じセット内の通信装置Ａ３を挿入して、メモリ１７６上に、図１８（ａ）に示すような通信装置Ａ３の番号、通信アドレス、共通鍵Ｋ１を持つ、スロット１７１対応の自通信装置情報テーブル１８０を生成し、また、通信装置Ａ０をスロット１７１に挿入して、メモリ１７６上に、図１８（ｂ）に示すような通信装置Ａ０の番号、通信アドレス、共通鍵Ｋ１を持つ、スロット１７１対応の送信先情報テーブル１８１を生成する。更に、端末装置１５０の送信先一覧テーブルに通信装置Ａ３の通信装置番号、通信アドレス、共通鍵Ｋ１を登録しておく。スロット１７２側についても同様の作業を行う。つまり、スロット１７２に通信装置Ｆ０と同じセット内の通信装置Ｆ３を挿入して、メモリ１７６上に、図１８（ｃ）に示すような通信装置Ｆ３の番号、通信アドレス、共通鍵Ｋ２を持つ、スロット１７２対応の自通信装置情報テーブル１８２を生成し、また、通信装置Ｆ０をスロット１７２に挿入して、メモリ１７６上に、図１８（ｄ）に示すような通信装置Ｆ０の番号、通信アドレス、共通鍵Ｋ２を持つスロット１７２対応の送信先情報テーブル１８３を生成する。更に、端末装置１６０の送信先一覧テーブルに通信装置Ｆ３の通信装置番号、通信アドレス、共通鍵Ｋ２を登録しておく。これにより、通信装置Ａ０と通信装置Ａ３との間がワイヤレス接続され、また通信装置Ｆ０と通信装置Ｆ３との間がワイヤレス接続される。

【００８０】

さて、通信装置Ａ０を持つ端末装置１５０から共通鍵Ｋ１で暗号化されたデー

タが通信装置Ａ３に送信されてくると、中継装置１７０の制御部１７５は、スロット１７１対応の自通信装置情報テーブル１８０の共通鍵Ｋ１によって暗号データを復号化し、スロット１７２対応の自通信装置情報テーブル１８２の共通鍵Ｋ２によって再び暗号化する。そして、その暗号化したデータに、送信元アドレスとしてスロット１７２対応の自通信装置情報テーブル１８２の通信アドレスを、送信先アドレスとしてスロット１７２対応の送信先情報テーブル１８３の通信アドレスを、それぞれ付加した送信データを通信装置Ｆ２によって、通信装置Ｆ０に送信する。このデータを受信した通信装置Ｆ０を持つ端末装置１６０は共通鍵Ｋ２で復号化する。これとは逆の中継も同様に行われる。

【００８１】

以上は中継専用の装置１７０を用いて異なるセットの通信装置間の接続を可能にしたが、端末装置自体に２つ以上のスロットと中継機能を持たせるようにしても良い。

【００８２】

なお、以上の各実施例では、通信装置に固有の番号を付記し、その通信装置の通信アドレスの下位アドレス部に前記番号を設定し、送信先選択画面でその番号を表示することで、どの通信装置がどの端末装置に挿入されているかをユーザに認識させた。しかし、このような方法に代えて、例えば、各端末装置に自通信装置の通信アドレス及び他通信装置の通信アドレスを登録した後、各端末装置が他通信装置の通信アドレスを送信先アドレス、自通信装置の通信アドレスを送信元アドレスに指定して、他の端末装置に装置名を問い合わせるメッセージを送信し、このメッセージを受信した端末装置が自端末装置の名前（例えば携帯端末装置であるとか、ＰＤＡであるとか等）を返信し、この名前を前記番号に代えて、或いは番号と共に送信先選択画面に表示するようにしても良い。

【００８３】

【発明の他の実施の形態】

これまでは、図１の携帯端末装置１ａ、ＰＤＡ１ｂ、ＰＣ１ｃをワイヤレス接続する構成について説明した。以下では、図１の携帯端末装置１ａ、ＰＤＡ１ｂ、ＰＣ１ｃから移動体通信サービスを利用する際の構成例について説明する。

【００８４】

図１９は移動体通信サービスを利用する際に使用する通信装置のセットを示し、４ａはＰＨＳシステム用、５ａはＰＤＣシステム用、６ａはＣＤＭＡシステム用の通信装置（以下、無線モジュールと称す）であり、それぞれ移動体通信システムを利用する際に端末装置のスロットに挿入して使用する。また、４ｂ、５ｂ、６ｂは、正規の無線モジュールが正規の端末装置以外で不正に使用されるのを防止するための認証用のキーモジュールであり、無線モジュール４ａ、５ａ、６ａに１対１に対応している。全ての無線モジュールおよびキーモジュールは、前述したワイヤレス接続用の通信装置と同じ規格で統一された同一の外形形状を有する。更に、無線モジュール４ａ、５ａ、６ａは、端末装置のスロットに挿入したときに装置外にはみ出る装置の一部分（図１９でハッチングを施した部分）が、利用できる移動体通信サービスの種類に応じた色で色付けされており、色を見れば、どの移動体通信サービス用の無線モジュールであるかが即座に認識できるようになっている。なお、無線モジュール４ａ、５ａ、６ａはスロット外にはみ出る必要は必ずしもなく、露出していれば良い。

【００８５】

無線モジュール４ａ、５ａ、６ａの構造は、図２に示したワイヤレス接続用の通信装置３ａ～３ｃと基本的に同じであり、図２０に示すように、筐体３０の両端にコネクタ３１およびアンテナ３２を有し、筐体３０内に、インタフェイス３３、制御部３４、メモリ３５、無線部３６および要素間を接続する信号線Ｌ１～Ｌ５並びに電源線３７を有している。但し、無線部３６は、無線モジュール４ａにあってはＰＨＳシステムに適合するよう設計され、無線モジュール５ａにあってはＰＤＣシステムに適合するよう設計され、無線モジュール６ａにあってはＣＤＭＡシステムに適合するよう設計されている。また、メモリ３５はＥＥＰＲＯＭ等の不揮発性メモリで構成され、何れも所定の認証用データが記憶されていると共に、ＰＨＳやＰＤＣの場合は課金コードも記憶されている。

【００８６】

またキーモジュール４ｂ、５ｂ、６ｂは、図２１に示すように、筐体４０の一端にコネクタ４１を有し、筐体４０内に、コネクタ４１に信号線Ｌ４１で接続さ

れたインタフェイス４２、これに信号線Ｌ４２で接続された制御部４３、これに信号線Ｌ４３で接続されたメモリ４４を有している。また、コネクタ４１を通じて端末装置側から供給される電力を各部に伝達する電源線４５がある。メモリ４４は認証に使用する所定の情報を記憶するＥＥＰＲＯＭ等の不揮発性メモリである。コネクタ４１とインタフェイス４２は、端末装置側のアダプタと機械的ないし電気的に接続するアダプタを構成する。制御部４３はＭＰＵおよび制御プログラムを記憶するＲＯＭ等で構成され、所定の認証処理を実行する。

【００８７】

例えば図１の携帯端末装置１ａをＰＨＳ電話機として利用する場合、ＰＨＳ用の無線モジュール４ａと組になっているキーモジュール４ｂをスロット２ａに挿入して、メモリ４４に記憶されている認証用のデータを携帯端末装置１ａ側に登録しておく。そして実際の利用時は、ＰＨＳ用の無線モジュール４ａをスロット２ａに挿入してＰＨＳシステムを利用する。このとき、無線モジュール４ａと携帯端末装置１ａとの間で相互に認証が行われる。認証が成功しない限り、無線モジュール４ａは使用できない。携帯端末装置１ａをＰＤＣ電話機、ＣＤＭＡ電話機として利用することもできる。その場合も、事前にキーモジュール５ｂ、６ｂに記憶された認証用データを携帯端末装置１ａ側に登録し、無線モジュール５ａ、６ａをスロット２ａに挿入した際、無線モジュール５ａ、６ａと携帯端末装置１ａとで相互に認証処理を行う。携帯端末装置１ａと同様の作業を行えば、無線モジュール４ａ、５ａ、６ａおよびキーモジュール４ｂ、５ｂ、６ｂを使ってＰＤＡ１ｂやＰＣ１ｃで、ＰＨＳシステム、ＰＤＡシステム、ＣＤＭＡシステムを利用することもできる。

【００８８】

キーモジュール４ｂ、５ｂ、６ｂは、それを使って認証用のデータを端末装置に一旦登録してしまえば普段は使わない。したがってキーモジュール４ｂ、５ｂ、６ｂを厳重に保管しておけば、ＰＨＳ、ＰＤＣ、ＣＤＭＡシステム用の無線モジュール４ａ、５ａ、６ａが盗難にあっても、悪用される心配がなくなり、様々な無線インフラを無線モジュールを差し替えるだけで安心して利用することが可能となる。

【００８９】

次に認証の具体例について、携帯端末装置１ａを例に以下説明する。

【００９０】

無線モジュール４ａ、５ａ、６ａを販売店で購入すると、それぞれ専用のキーモジュール４ｂ、５ｂ、６ｂが添付される。それぞれのモジュールには、認証に使うデータとして図２２に示すようなデータが内部のメモリ３５、４４に記憶されている。認証用データは、モジュールＩＤ、認証コードKEY_{ID}、暗号関数f_{ID}（ｘ）、その逆暗号関数f_{ID}^{-1}（ｘ）から成り、無線モジュールとそのキーモジュールとには同じユニークなモジュールＩＤ、認証コードKEY_{ID}が共に記憶され、逆暗号関数f_{ID}^{-1}（ｘ）は無線モジュール側に、その暗号関数f_{ID}（ｘ）はキーモジュール側に記憶される。認証コードKEY_{ID}、暗号関数f_{ID}（ｘ）、逆暗号関数f_{ID}^{-1}（ｘ）も、無線モジュールとキーモジュールの組毎にユニークなものとなっている。

【００９１】

最初に、キーモジュールに記憶された認証用データを携帯端末装置１ａに登録する。携帯端末装置１ａのキーパッド１０１の操作でキーモジュール登録処理を起動すると、制御部１０４は図２３に示す処理を開始する。先ず、スロット２ａにキーモジュールを挿入する促進メッセージを表示器１０２に表示する（Ｓ１０１）。ユーザが例えばＰＨＳシステム用のキーモジュール４ｂをスロット２ａに挿入すると、携帯端末装置１ａに内蔵の電源１０８からスロット２ａを通じてキーモジュール４ｂに電力が供給されて各部が動作可能となる。制御部１０４はインタフェイス１０７、ソケット１０９、コネクタ４１、インタフェイス４２および制御部４３を通じてメモリ４４に記憶されたモジュールＩＤ１、認証コードKEY_{ID1}、暗号関数f_{ID1}（ｘ）を読み込み（Ｓ１０２）、認証テーブルに保存する（Ｓ１０３）。

【００９２】

次に制御部１０４は他に登録するキーモジュールがあるか否かを表示器１０２にメッセージを表示してユーザに問い合わせ、他のキーモジュールがある場合（Ｓ１０４でＮＯ）、ステップＳ１０１に戻って上述した処理を繰り返す。ユーザ

がＰＨＳシステム用以外にＰＤＣシステム用やＣＤＭＡシステム用のモジュールを持っている場合、それらのキーモジュールをスロット２ａに挿入することで、認証用データを携帯端末装置１ａに登録する。登録するキーモジュールが他になければ（Ｓ１０４でＹＥＳ）、制御部１０４は処理を終了する。

【００９３】

図２４に携帯端末装置１ａのメモリ１０６上に設けられた認証テーブル２０１の内容例を示す。この例では、ＰＨＳ用の認証データ２０２、ＰＤＣ用の認証データ２０３、ＣＤＭＡ用の認証データ２０４の３種類が設定されている。なお、エントリ２０５～２０７は実際の認証時に乱数が格納される部分であり、キーモジュールの登録時はＮＵＬＬになっている。

【００９４】

次に、無線モジュールを使用して携帯端末装置１ａから移動体通信サービスを利用する際の認証処理について説明する。

【００９５】

携帯端末装置１ａのキーパッド１０１の操作で無線モジュール登録処理を起動すると、制御部１０４は図２５に示す処理を開始する。先ず、スロット２ａに無線モジュールを挿入する促進メッセージを表示器１０２に表示する（Ｓ１１１）。ユーザが例えばＰＨＳシステム用の無線モジュール４ａをスロット２ａに挿入すると、携帯端末装置１ａに内蔵の電源１０８からスロット２ａを通じて無線モジュール４ａに電力が供給されて各部が動作可能となる。制御部１０４は、無線モジュール４ａからモジュールＩＤが送られてくるのを待つ。

【００９６】

無線モジュール４ａの制御部３４は、電源が投入されると図２６に示す認証処理を開始する。先ず、メモリ３５に記憶されたモジュールＩＤ１を読み取って、インタフェイス３３、コネクタ３１を介して携帯端末装置１ａに送出する（Ｓ１３１）。そして、携帯端末装置１ａから応答データが送られてくるのを待つ。

【００９７】

携帯端末装置１ａの制御部１０４は、このモジュールＩＤ１をソケット１０９、インタフェイス１０７を通じて受け取ると（Ｓ１１２）、モジュールＩＤ１で

図２４の認証テーブル２０１を検索し、同じモジュールＩＤ１が登録されているか否かを調べる（Ｓ１１３）。同じモジュールＩＤ１が登録されていない場合（Ｓ１１３でＮＯ）、認証失敗となる（Ｓ１１４）。認証が失敗すると、制御部１０４は当該無線モジュール４ａを不正なモジュールと判断し、当該無線モジュール４ａを使用した制御を行わない。他方、同じモジュールＩＤ１が登録されていた場合（Ｓ１１３でＹＥＳ）、それと組になって登録されている認証コードKEY_{ID1}、暗号関数$f_{ID1}(x)$を認証テーブル２０１から読み取り（Ｓ１１５）、乱数発生プログラム等によって乱数Ｒａｎｄを生成し（Ｓ１１６）、KEY_{ID1}と乱数Ｒａｎｄを連結したデータを暗号関数$f_{ID1}(x)$で暗号化し（Ｓ１１７）、無線モジュール４ａに暗号化データを送出する（Ｓ１１８）。そして、無線モジュール４ａから応答データが送られてくるのを待つ。なお、発生した乱数Ｒａｎｄは、後の処理のために認証テーブルに記憶しておく。

【００９８】

無線モジュール４ａの制御部３４は、暗号化データを携帯端末装置１ａから受け取ると（Ｓ１３２）、その暗号化データを逆暗号関数$f_{ID1}^{-1}(x)$で復号し、認証コードKEY_{ID1}と乱数Ｒａｎｄを得る（Ｓ１３３）。そして、復号化して得た認証コードKEY_{ID1}がメモリ３５に記憶されている認証コードKEY_{ID1}と一致するか否かを調べ（Ｓ１３４）、一致しなければ異常コードを携帯端末装置１ａに送出し（Ｓ１３５）、処理を終了する。他方、一致すれば、前記復号化して得た乱数Ｒａｎｄを逆暗号関数$f_{ID1}^{-1}(x)$で暗号化し（Ｓ１３６）、携帯端末装置１ａに送出して（Ｓ１３７）、処理を終了する。

【００９９】

携帯端末装置１ａの制御部１０４は、無線モジュール４ａからの応答データを受け取ると（Ｓ１１９）、それが異常コードであった場合（Ｓ１２０）、認証失敗とする（Ｓ１１４）。応答内容が異常コードでない場合、応答内容を暗号関数$f_{ID1}(x)$で復号し、乱数Ｒａｎｄを得る（Ｓ１２１）。そして、この復号化した得た乱数ＲａｎｄとステップＳ１１６で自ら生成した乱数Ｒａｎｄとが一致するか否かを調べ（Ｓ１２２）、一致しない場合、認証失敗とする（Ｓ１１４）。一致した場合は認証成功となる（Ｓ１２３）。以後、制御部１０４は、当該無

線モジュール４ａを使ったＰＨＳシステムの利用を可能とする。認証成功の場合、制御部１０４は、携帯端末装置１ａが若しロック状態であればそれを解除し（Ｓ１２４）、所定の監視処理を起動し（Ｓ１２５）、図２５の処理を終了する。ステップＳ１２４、Ｓ１２５の詳細については後述する。

【０１００】

以上はＰＨＳシステムの無線モジュール４ａを使う場合の携帯端末装置１ａと無線モジュール間の相互認証について説明したが、ＰＤＣシステムの無線モジュール５ａ、ＣＤＭＡシステムの無線モジュール６ａを使用する場合にも、携帯端末装置１ａと無線モジュール間で同様な相互認証が行われ、認証成功時にのみ当該無線モジュール５ａ、６ａの利用が可能となる。また、携帯端末装置１ａを例にしてキーモジュールの登録と無線モジュール使用時の認証処理を説明したが、図２３および図２５に示されるような機能はＰＤＡ１ｂおよびＰＣ１ｃのＭＰＵ１１１によっても提供されているため、携帯端末装置１ａと同じ作業を実施することにより、ＰＤＡ１ｂおよびＰＣ１ｃでも無線モジュール４ａ、５ａ、６ａを使用した移動体通信サービスの利用が可能である。

【０１０１】

次に、図２５のステップＳ１２４、Ｓ１２５について、携帯端末装置１ａの場合を例に説明する。ＰＤＡ１ｂ、ＰＣ１ａの場合も同様である。

【０１０２】

ステップＳ１２５で起動される監視処理の一例を図２７に示す。この監視処理は携帯端末装置１ａの電源スイッチのオン、オフにかかわらず実行される。監視処理が起動されると、制御部１０４はスロット２ａから通信装置（無線モジュール）が外されたかどうか、キーパッド１０１から所定のキー操作によって監視停止が指示されたかどうかを監視する（Ｓ１４１、Ｓ１４２）。スロット２ａから通信装置が外されたかどうかは、例えばソケット１０９の所定の端子がコネクタ３１に接続されているときの電気的な状態を示すか否かや、通信装置の制御部と交信を試みる等の任意の方法が利用できる。

【０１０３】

スロット２ａから通信装置が外された場合（Ｓ１４１でＹＥＳ）、制御部１０

４は、携帯端末装置１ａに対するユーザの一切の入力を無効とするロック状態とする（Ｓ１４３）。従って、キーパッド１０１による操作は一切行えず、メモリ１０６に記憶された電話帳などの情報を表示器１０２に表示させることもできなくなる。ＰＡＤ１ｂのようにタブレット１２１を有する装置ではペン入力も無効となり、マウスを有する場合にはマウス入力も無効となる。その後、制御部１０４は、スロット２ａに通信装置（無線モジュール）が挿入されたか否かを監視し（Ｓ１４４）、挿入されたら、図２５に示した相互認証処理におけるステップＳ１１２へと進む。この結果、外された通信装置が再びスロット２ａに挿入されると図２５に示した相互認証処理が実施される。そして、認証が成功すると、ステップＳ１２４において携帯端末装置１ａのロック状態が解除される。これによって、ユーザによる入力操作が可能となる。

【０１０４】

他方、監視処理中に監視停止の指示があった場合（Ｓ１４２でＹＥＳ）、制御部１０４は図２７の監視処理を終了する。この後、スロット２ａから通信装置を外しても装置はロック状態にならない。これは、携帯端末装置１ａに対する新たなキーモジュールの登録作業や前述したワイヤレス接続用の通信装置の登録作業などを可能にするためである。

【０１０５】

図２８は移動体通信サービスを利用する際に使用する通信装置の別のセットの例を示し、７ａはお父さん用の無線モジュール、７ｂはそのキーモジュール、８ａはお母さん用の無線モジュール、８ｂはそのキーモジュール、９ａは自分用の無線モジュール、９ｂはそのキーモジュールである。無線モジュール７ａ、８ａ、９ａは、所定の移動体通信サービス用（例えばＰＨＳシステム用）のもので、端末装置のスロットに挿入して使用する。また、キーモジュール７ａ、８ａ、９ａは、前述したキーモジュール４ｂ、５ｂ、６ｂと同じ目的のために使用するモジュールである。全てのモジュールは、前述したキーモジュール４ｂ、５ｂ、６ｂと同じ規格で統一された同一の外形形状を有する。更に、無線モジュール７ａ、８ａ、９ａは、端末装置のスロットに挿入したときに装置外にはみ出る部分（図２８でハッチングを施した部分）が、利用する個人に応じた色で色付けされて

おり、色を見れば、どの人の無線モジュールであるかが即座に認識できるようになっている。

【０１０６】

特定のプロバイダーに、申請者各員毎の住所、氏名、パスワード等の所定の事項を記載した申込書を郵送ないしインターネット経由で送信すると、プロバイダーから各員用の無線モジュールとキーモジュールのセットが送られてくる。図２８に示したモジュールのセットは、このようにして購入したもので、個々の無線モジュール７ａ、８ａ、９ａのメモリ３５には、当該プロバイダーに接続するために必要な一切の情報（プロバイダー接続情報と称す）が事前に記憶されている。プロバイダー接続情報には、プロバイダー側が各員に付与したユーザ名、各員が申請したパスワード、最寄りのアクセスポイントの電話番号等が含まれる。使用に際しては、前述と同様にキーモジュール７ｂ、８ｂ、９ｂに記憶された認証用データを例えば携帯端末装置１ａに登録し、次いで、個人の無線モジュール７ａまたは８ａまたは９ａを携帯端末装置１ａのスロット２ａに挿入し、認証を得た後、利用する。インターネットを利用する場合、無線モジュール７ａ、８ａ、９ａに記憶されたプロバイダー接続情報が利用される。

【０１０７】

図２９に携帯端末装置１ａのスロット２ａに例えば無線モジュール７ａを挿入して、インターネットに接続する際の処理の一例を示す。ユーザが携帯端末装置１ａのキーパッド１０１の操作で制御部１０４が有するブラウザ機能を起動すると、ブラウザが立ち上がる（Ｓ１５１）。次に制御部１０４は、スロット２ａに挿入された無線モジュール７ａのメモリ３５からプロバイダー接続情報を読み出し、メモリ１０６に記憶する（Ｓ１５２）。次に、パスワードの入力を促すメッセージを表示器１０２に表示してユーザからパスワードを入力させ（Ｓ１５３）、メモリ１０６に記憶したプロバイダー接続情報中のパスワードと比較する（Ｓ１５４）。パスワードが不一致のときはエラー処理を行い、一致した場合は、メモリ１０６に記憶したプロバイダー接続情報中の電話番号を用いて無線モジュール７ａからアクセスポイントに発呼し、ユーザＩＤおよびパスワードを送ってプロバイダーに接続する（Ｓ１５５）。以後、ユーザが指定するＵＲＬに従ってイ

ンターネット上のホームページをアクセスする。

【０１０８】

以上は無線モジュール７ａを用いたが、他の無線モジュール８ａ、９ａに差し替えれば他の個人もインターネットを即利用することができる。また、携帯端末装置１ａだけでなく、ＰＤＡ１ｂやＰＣ１ｃのスロットに挿入することで、これらからもインターネットに接続することができる。

【０１０９】

なお、以上の説明では、ユーザからのブラウザ起動の指示を待ってプロバイダーに接続したが、図２９の処理を図２５のステップＳ１２５の直後に自動的に実行することにより、無線モジュール７ａ、８ａ、９ａを端末装置のスロットに挿入すれば、プロバイダーに即接続される構成にすることができる。

【０１１０】

【発明の効果】

以上説明したように本発明によれば、以下のような効果が得られる。

【０１１１】

色分けされた様々な通信装置を差し替えることで様々な無線インフラに対応でき、且つ現在どのような通信装置を使用しているかを端末装置のスロットに通信装置が挿入された状態で外部から極めて容易に確認することができる。

【０１１２】

通信装置と同形状のキーモジュールによって認証用のデータを端末装置に一旦登録しておけば、通信装置を挿入する都度、パスワードなどをユーザが一々入力しなくても通信装置と端末装置間で認証処理が自動的に行われるため、他人による通信装置の悪用を防止するために必要なユーザの作業量を削減することができる。また、登録には必ずキーモジュールが必要であるため、パスワード入力より安全性が高い。

【０１１３】

端末装置と通信装置との間で認証が成立した後、通信装置がスロットから取り出されたとき、端末装置を利用者からの入力を一切受け付けないロック状態とする構成にあっては、通信装置に鍵（キー）の機能を持たせることができる。

【０１１４】

特定のプロバイダーに接続するのに必要な情報を記憶するメモリを備えた通信装置によれば、通信装置を購入すれば直ちにインターネットのプロバイダーへの接続が可能になり、インターネットを手軽に利用できる通信装置を提供できる。

【０１１５】

端末間をワイヤレス接続する通信装置をその伝送速度に応じて色分けした構成にあっては、現在どのような伝送速度の通信装置を使用しているかを端末装置のスロットに通信装置が挿入された状態で外部から極めて容易に確認することができる。

【０１１６】

本発明の通信装置セット及び端末間ワイヤレス接続方法によれば、同じセットの通信装置を端末装置のスロットに挿入するといった簡単な作業を行うだけで、通信アドレスやデータ暗号化用の鍵などの設定が行え、複数の端末間を手軽にワイヤレス接続することができる。

【図面の簡単な説明】

【図１】

本発明の一実施の形態を示すシステム構成図である。

【図２】

ワイヤレス接続用の通信装置の構成例を示すブロック図である。

【図３】

携帯端末装置の構成例を示すブロック図である。

【図４】

ＰＤＡの構成例を示すブロック図である。

【図５】

ユーザが購入した１セット分の通信装置の外観の概略と記憶情報の一例を示す図である。

【図６】

端末装置へのワイヤレス接続用通信装置の登録処理の第１の例を示すフローチ

ャートである。

【図７】

ワイヤレス接続用通信装置の登録処理によって生成される自通信装置情報テーブル、送信先一覧テーブル、送信先選択画面の例を示す図である。

【図８】

ワイヤレス接続用通信装置間で授受される送信データのフォーマット例を示す図である。

【図９】

ユーザが購入した１セット分の通信装置の外観の概略と記憶情報の他の例を示す図である。

【図１０】

ユーザが購入した１セット分の通信装置の外観の概略と記憶情報の更に別の例を示す図である。

【図１１】

端末装置へのワイヤレス接続用通信装置の登録処理の第２の例を示すフローチャートである。

【図１２】

ワイヤレス接続用通信装置の登録処理によって生成される自通信装置情報テーブル、送信先一覧テーブル、送信先選択画面の他の例を示す図である。

【図１３】

端末装置へのワイヤレス接続用通信装置の登録処理の第３の例を示すフローチャートである。

【図１４】

端末装置へのワイヤレス接続用通信装置の登録処理の第４の例を示すフローチャートである。

【図１５】

ワイヤレス接続する通信装置群の一例を示す図である。

【図１６】

端末装置へのワイヤレス接続用通信装置の登録処理の第５の例を示すフローチ

ャートである。

【図１７】

中継装置を使って異なるセットの通信装置間で通信する構成例を示すブロック図である。

【図１８】

中継装置の各スロット毎に生成される自通信装置情報テーブル、送信先情報テーブルの例を示す図である。

【図１９】

移動体通信サービスを利用する際に使用する通信装置のセットの概略を示す図である。

【図２０】

移動体通信サービスを利用する際に使用する通信装置の構成例を示すブロック図である。

【図２１】

キーモジュールの構成例を示すブロック図である。

【図２２】

無線モジュールおよびキーモジュールに記憶されている認証用データの例を示す図である。

【図２３】

端末装置へのキーモジュールによる認証用データの登録処理の一例を示すフローチャートである。

【図２４】

端末装置のメモリ上に設けられた認証テーブルの内容例を示す図である。

【図２５】

端末装置側の認証処理の一例を示すフローチャートである。

【図２６】

無線モジュール側の認証処理の一例を示すフローチャートである。

【図２７】

端末装置側が認証成立時に起動する監視処理の一例を示すフローチャートであ

る。

【図２８】

移動体通信サービスを利用する際に使用する通信装置の別のセットの概略を示す図である。

【図２９】

端末装置から無線モジュールを使用してインターネットに接続する際の処理の一例を示すフローチャートである。

【符号の説明】

１ａ…携帯端末装置

１ｂ…ＰＤＡ

１ｃ…ＰＣ

２ａ～２ｃ…スロット

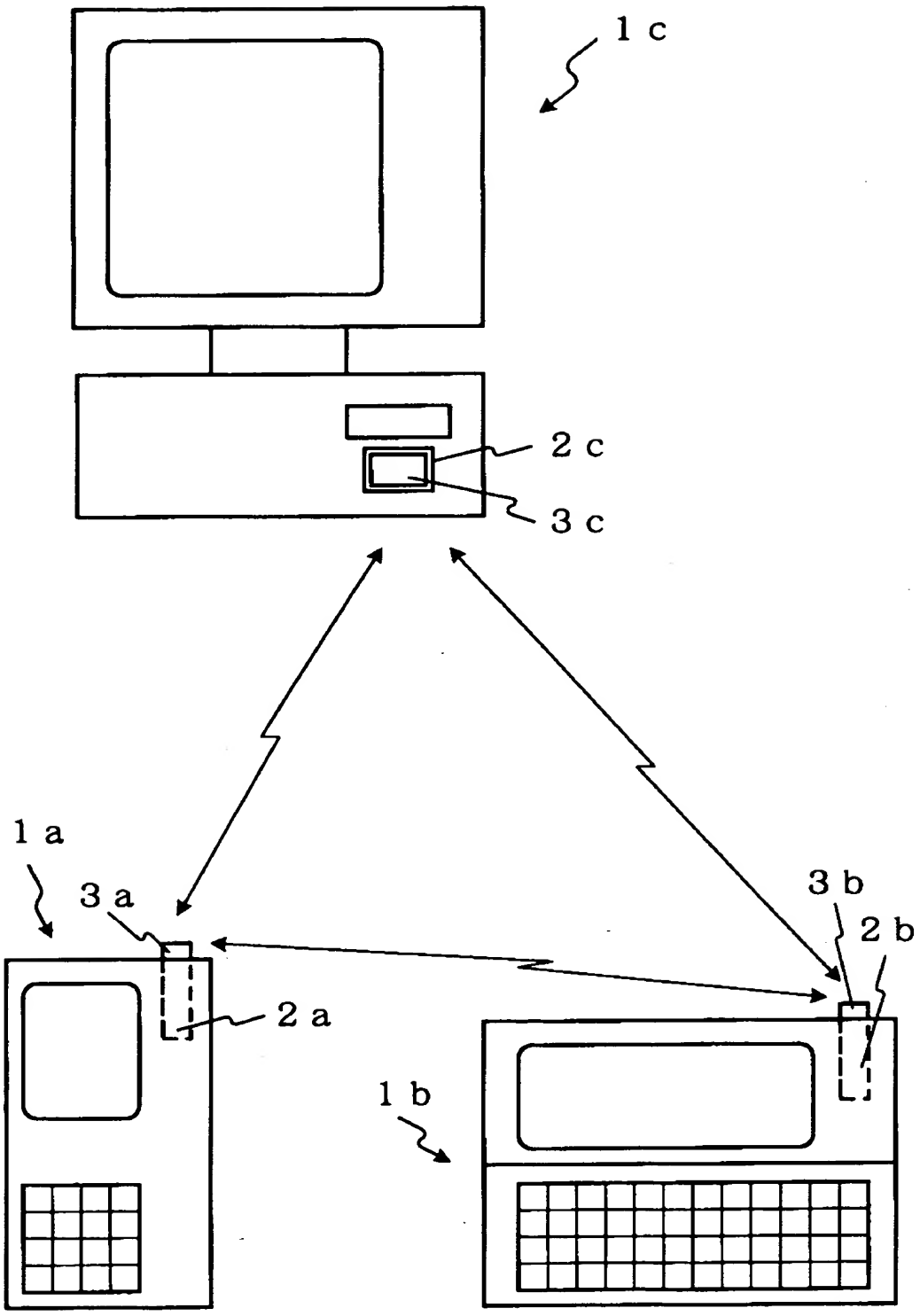
３ａ～３ｃ…ワイヤレス接続用の通信装置

４ａ～９ａ…移動体通信サービス接続用の無線モジュール（通信装置）

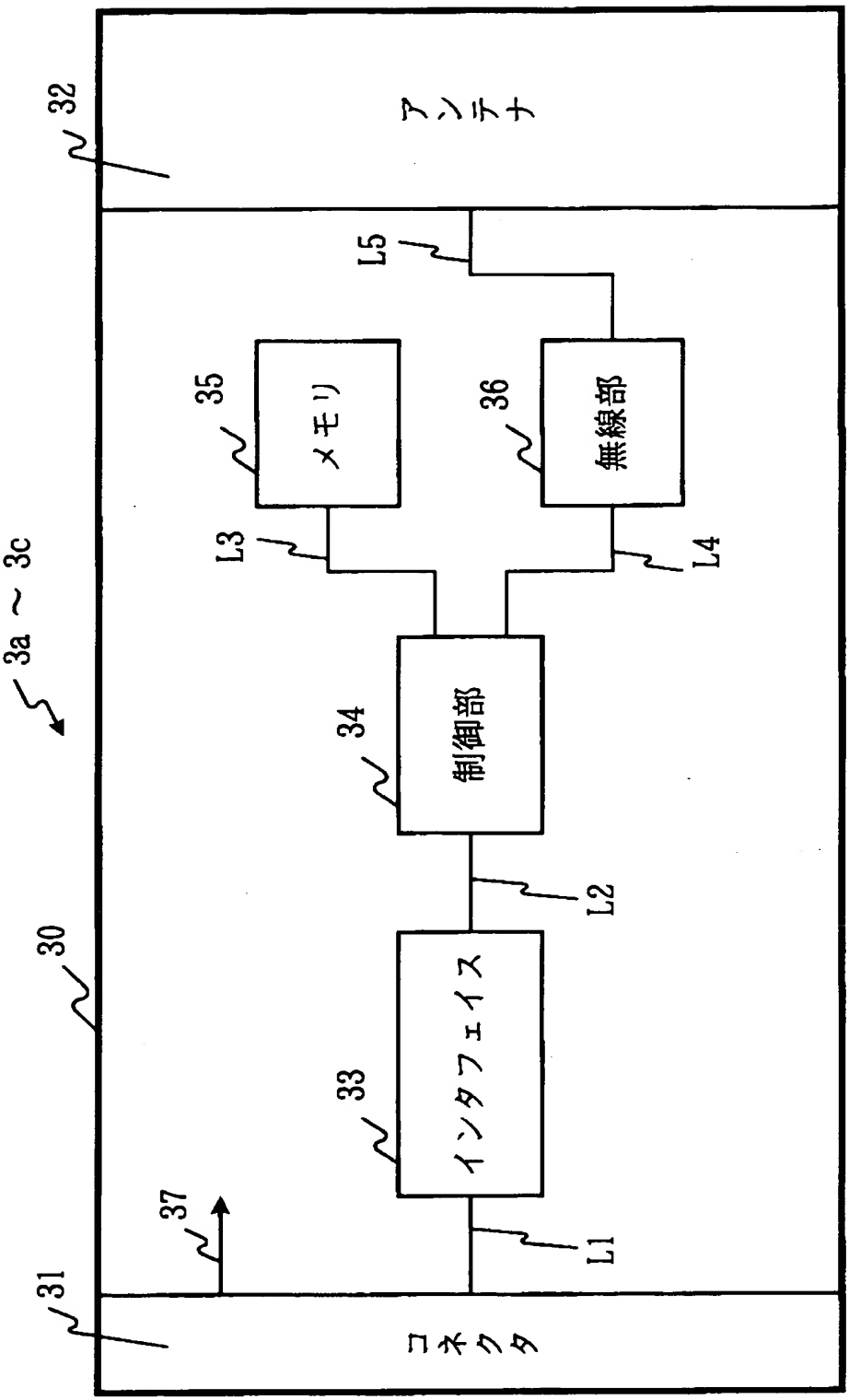
４ｂ～９ｂ…キーモジュール

【書類名】　　図面

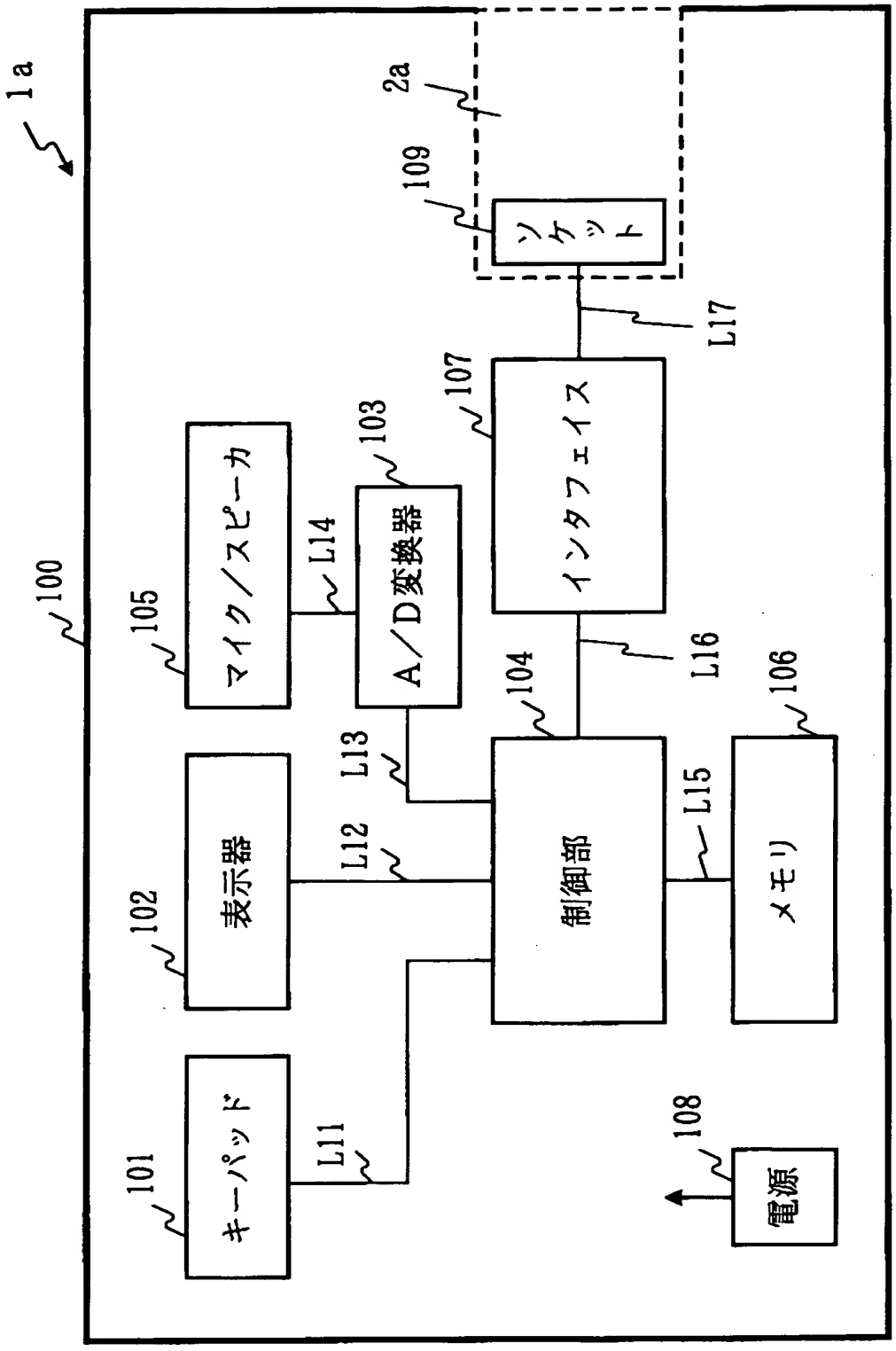
【図１】



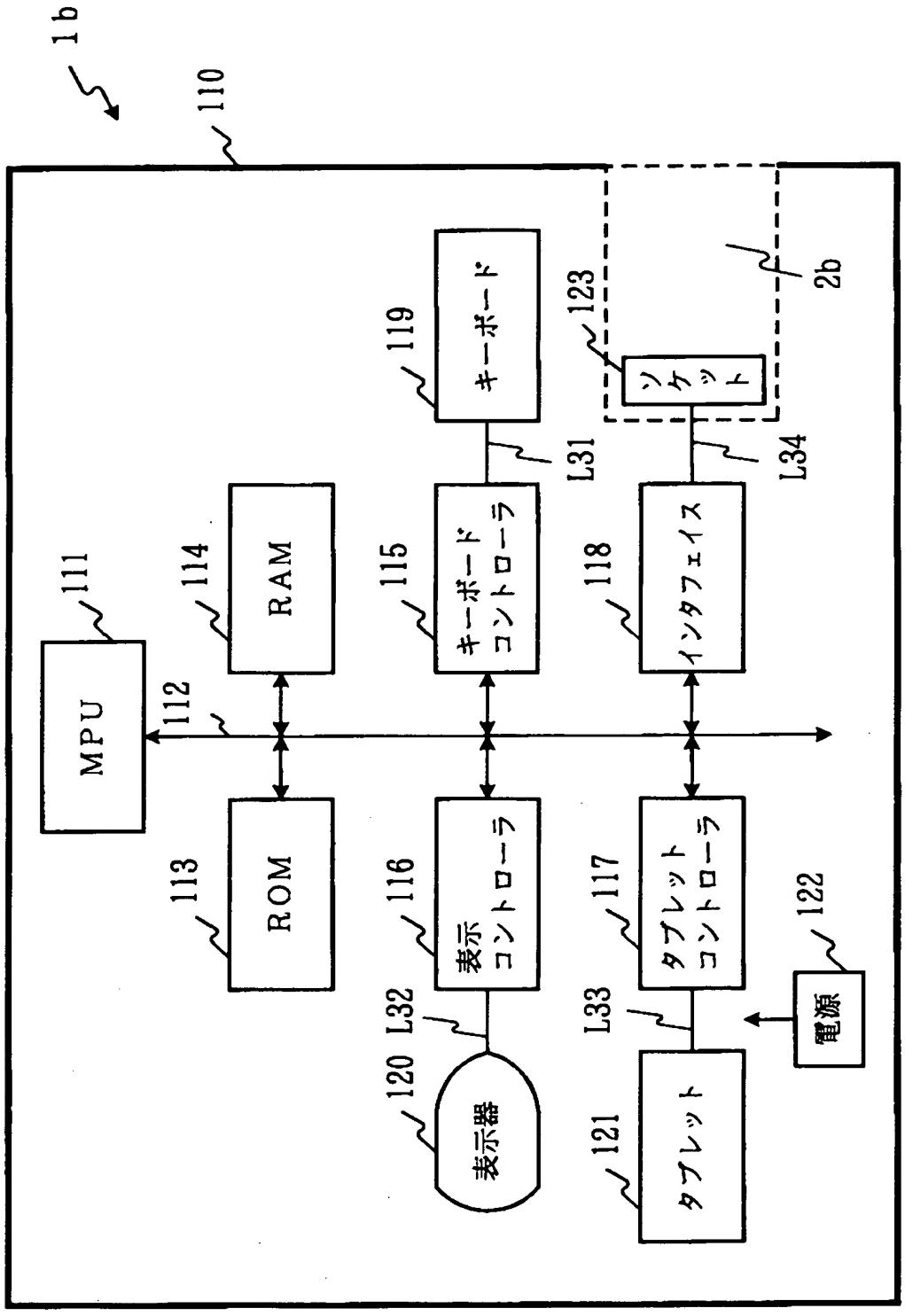
【図２】


アンテナ
32
L5
メモリ
35
無線部
36
L3
L4
3a ～ 3c
制御部
34
L2
30
インタフェース
33
37
L1
31
コネクタ

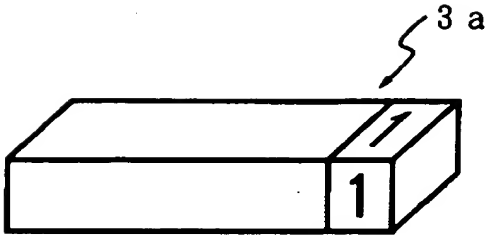
【図３】


1a
100
101
キーパッド
102
表示器
103
A／D変換器
104
制御部
105
マイク／スピーカ
106
メモリ
107
インタフェース
108
電源
109
ソケット
2a
L11
L12
L13
L14
L15
L16
L17

【図４】


1b
110
MPU
111
RAM
114
ROM
113
112
キーボード
119
キーボード
コントローラ
115
表示
コントローラ
116
表示器
120
タブレット
121
タブレット
コントローラ
117
インタフェイス
118
ソケット
123
2b
L31
L32
L33
L34
電源
122

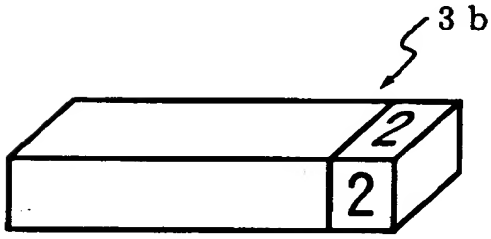
【図５】



自通信装置３ａの通信アドレス

他通信装置３ｂ，３ｃの通信アドレス

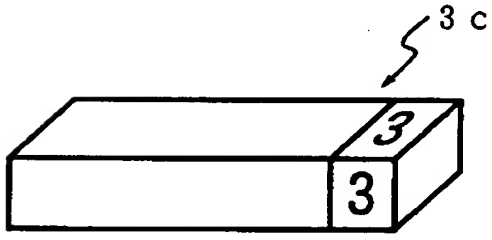
共通鍵Ｋ



自通信装置３ｂの通信アドレス

他通信装置３ａ，３ｃの通信アドレス

共通鍵Ｋ

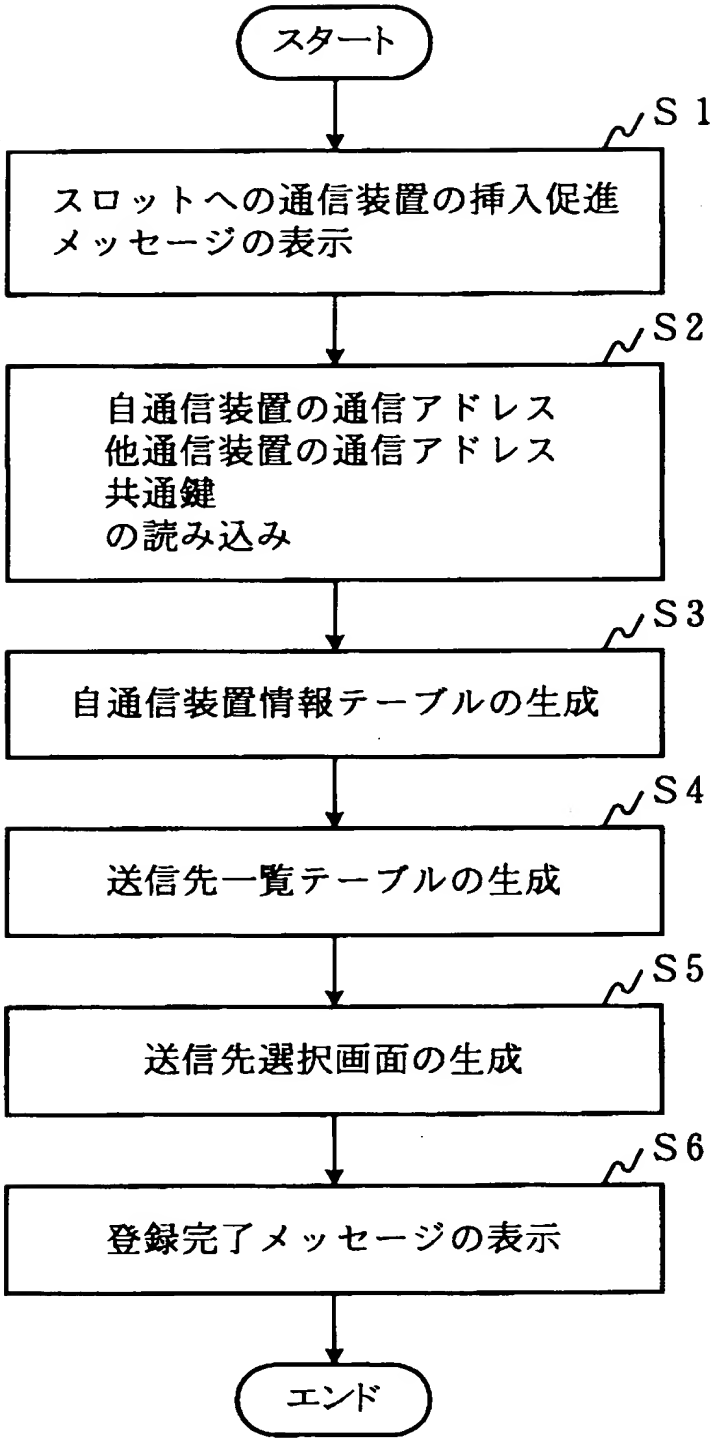


自通信装置３ｃの通信アドレス

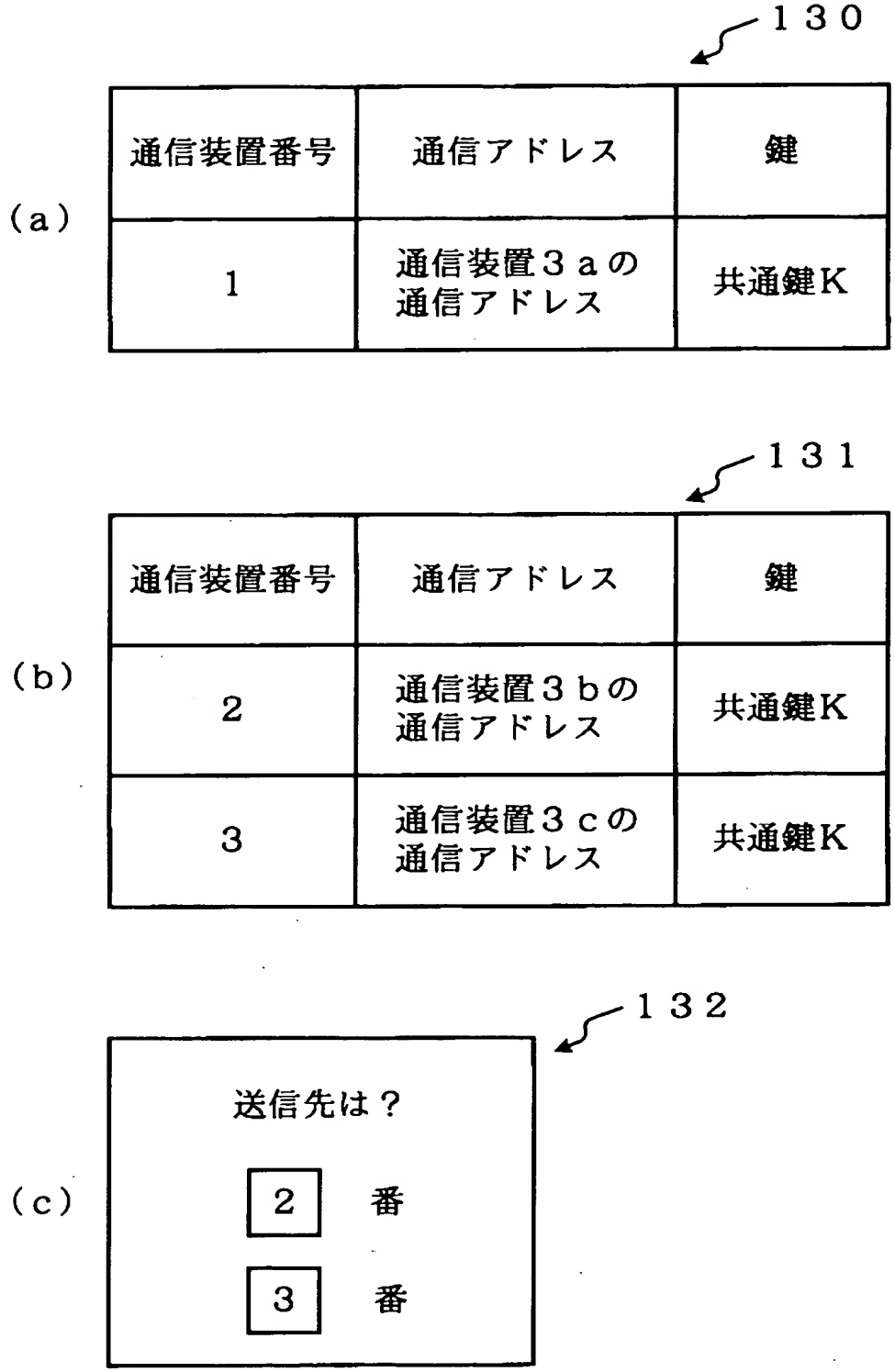
他通信装置３ａ，３ｂの通信アドレス

共通鍵Ｋ

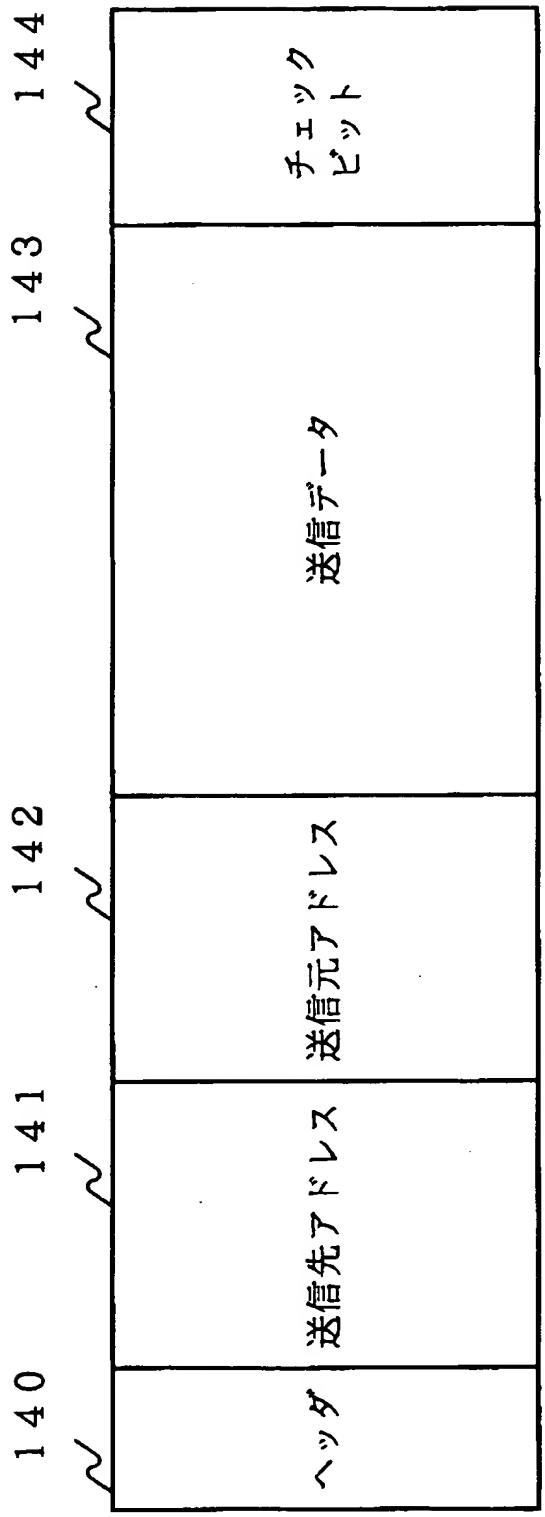
【図６】


スタート
S１
スロットへの通信装置の挿入促進
メッセージの表示
S２
自通信装置の通信アドレス
他通信装置の通信アドレス
共通鍵
の読み込み
S３
自通信装置情報テーブルの生成
S４
送信先一覧テーブルの生成
S５
送信先選択画面の生成
S６
登録完了メッセージの表示
エンド

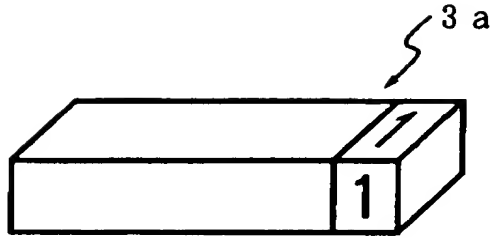
【図７】


１３０
通信装置番号
通信アドレス
鍵
１
通信装置３ａの通信アドレス
共通鍵Ｋ
（ａ）
１３１
通信装置番号
通信アドレス
鍵
２
通信装置３ｂの通信アドレス
共通鍵Ｋ
３
通信装置３ｃの通信アドレス
共通鍵Ｋ
（ｂ）
１３２
送信先は？
２ 番
３ 番
（ｃ）

【図８】



【図９】

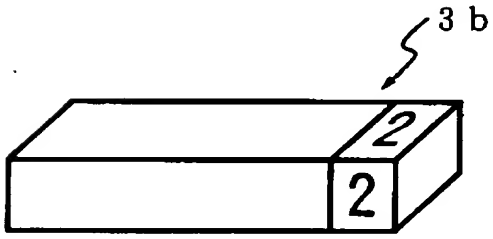


自通信装置３ａの通信アドレス

他通信装置３ｂ，３ｃの通信アドレス

自通信装置３ａの秘密鍵

他通信装置３ｂ，３ｃの公開鍵

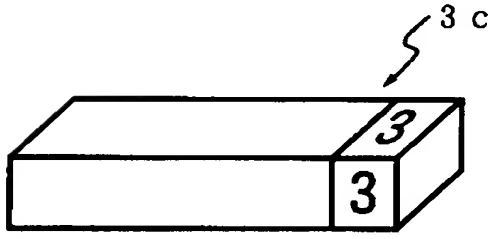


自通信装置３ｂの通信アドレス

他通信装置３ａ，３ｃの通信アドレス

自通信装置３ｂの秘密鍵

他通信装置３ａ，３ｃの公開鍵



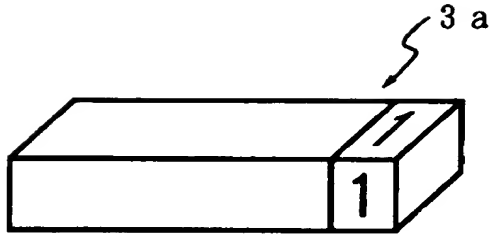
自通信装置３ｃの通信アドレス

他通信装置３ａ，３ｂの通信アドレス

自通信装置３ｃの秘密鍵

他通信装置３ａ，３ｂの公開鍵

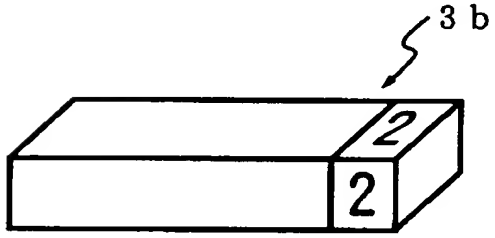
【図１０】



自通信装置３ａの通信アドレス

自通信装置３ａの秘密鍵

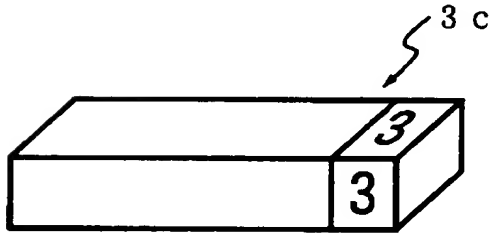
自通信装置３ａの公開鍵



自通信装置３ｂの通信アドレス

自通信装置３ｂの秘密鍵

自通信装置３ｂの公開鍵

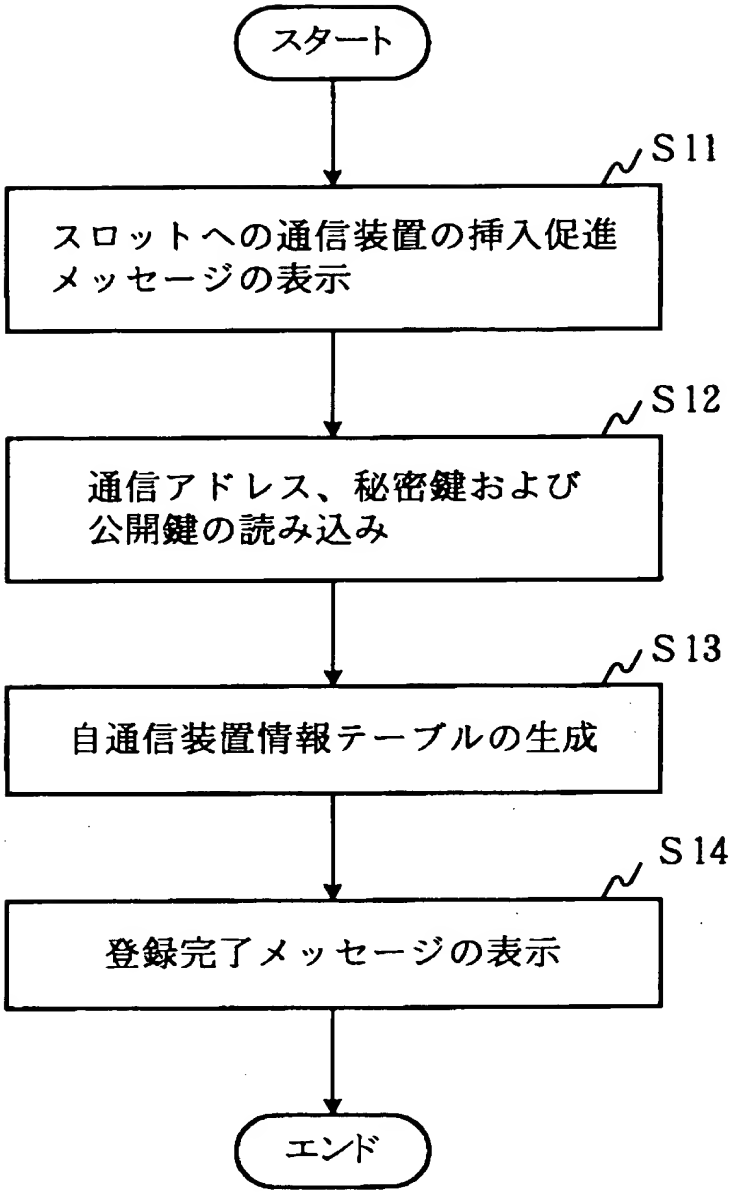


自通信装置３ｃの通信アドレス

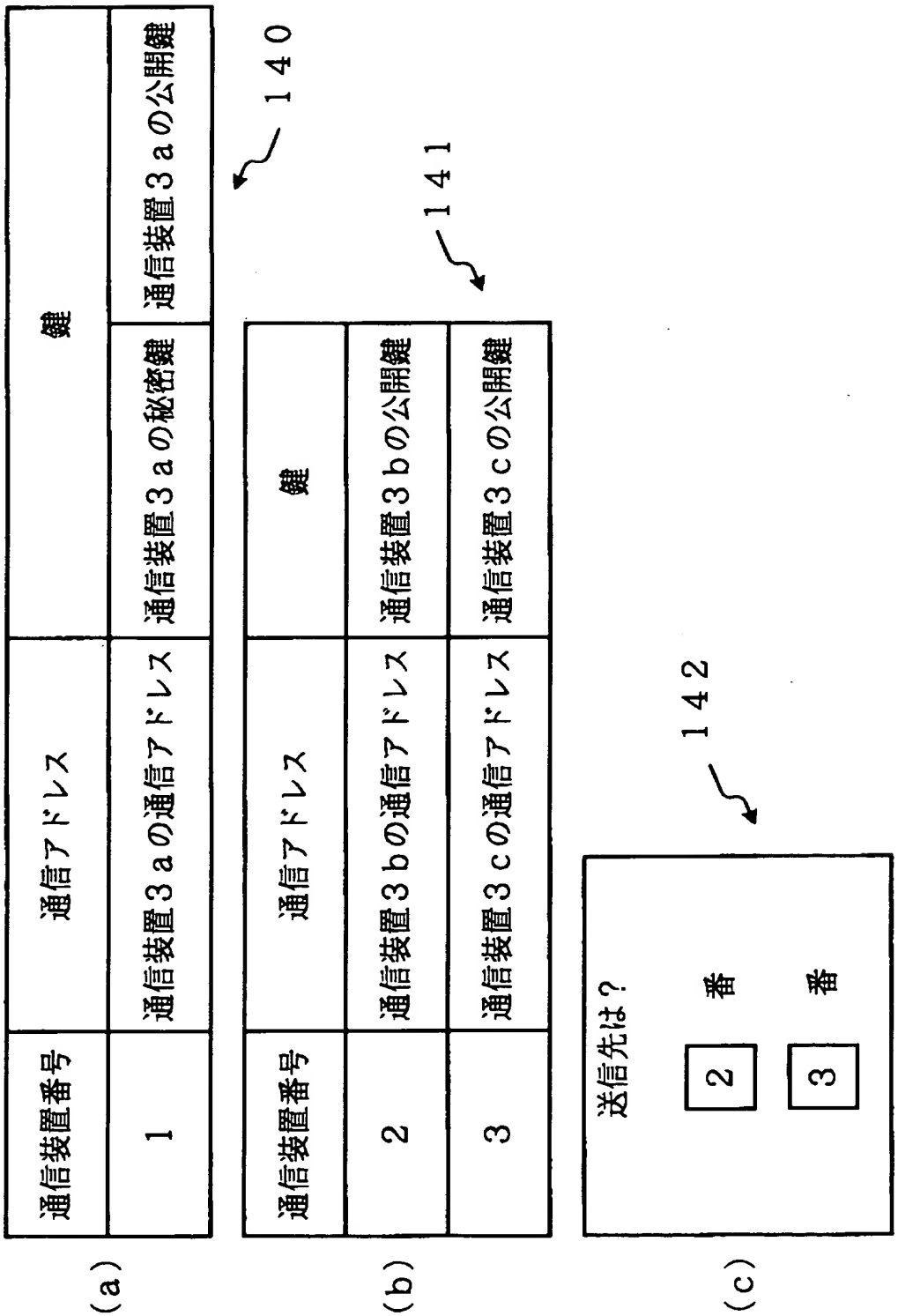
自通信装置３ｃの秘密鍵

自通信装置３ｃの公開鍵

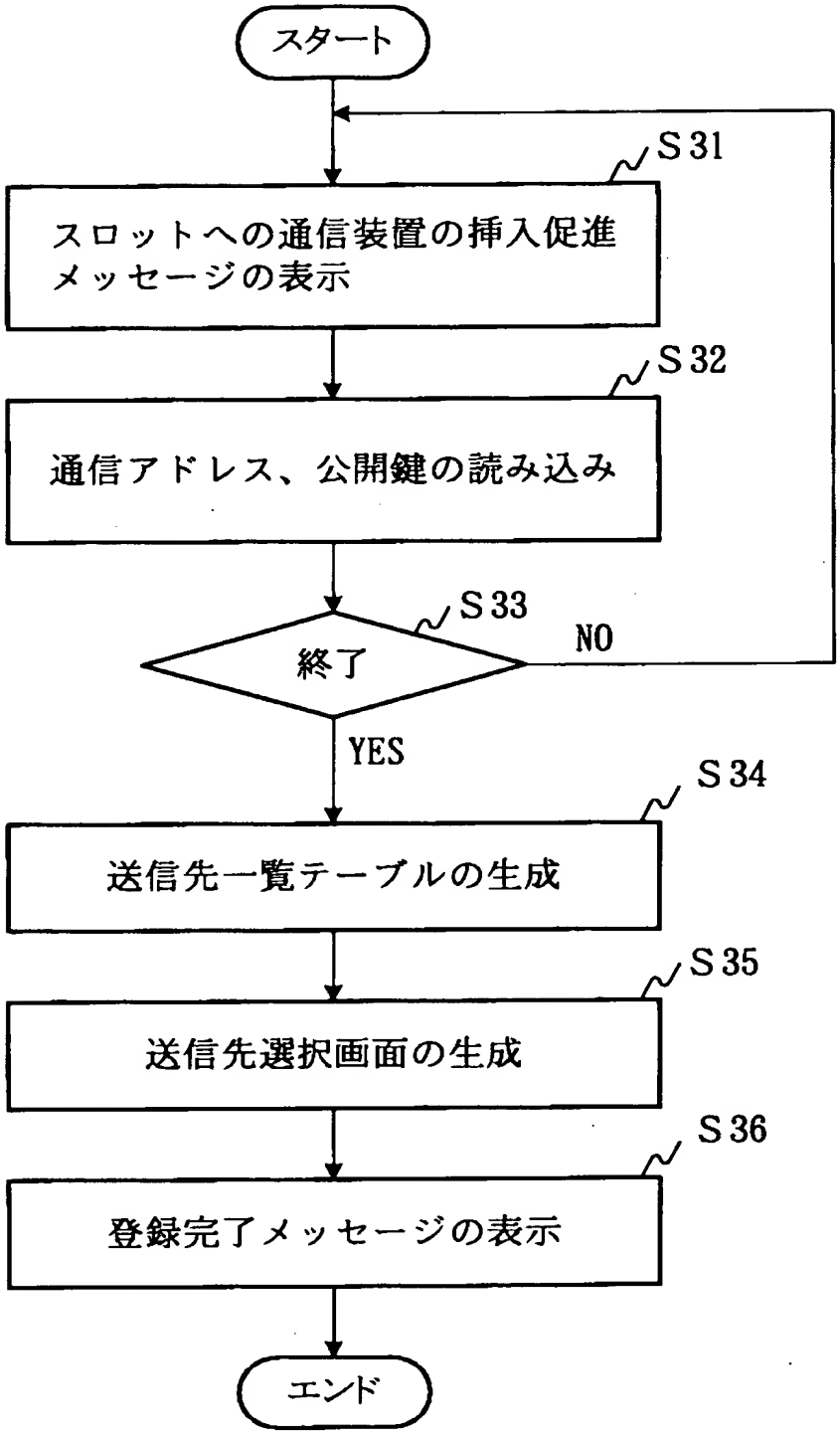
【図１１】


スタート
S11
スロットへの通信装置の挿入促進メッセージの表示
S12
通信アドレス、秘密鍵および公開鍵の読み込み
S13
自通信装置情報テーブルの生成
S14
登録完了メッセージの表示
エンド

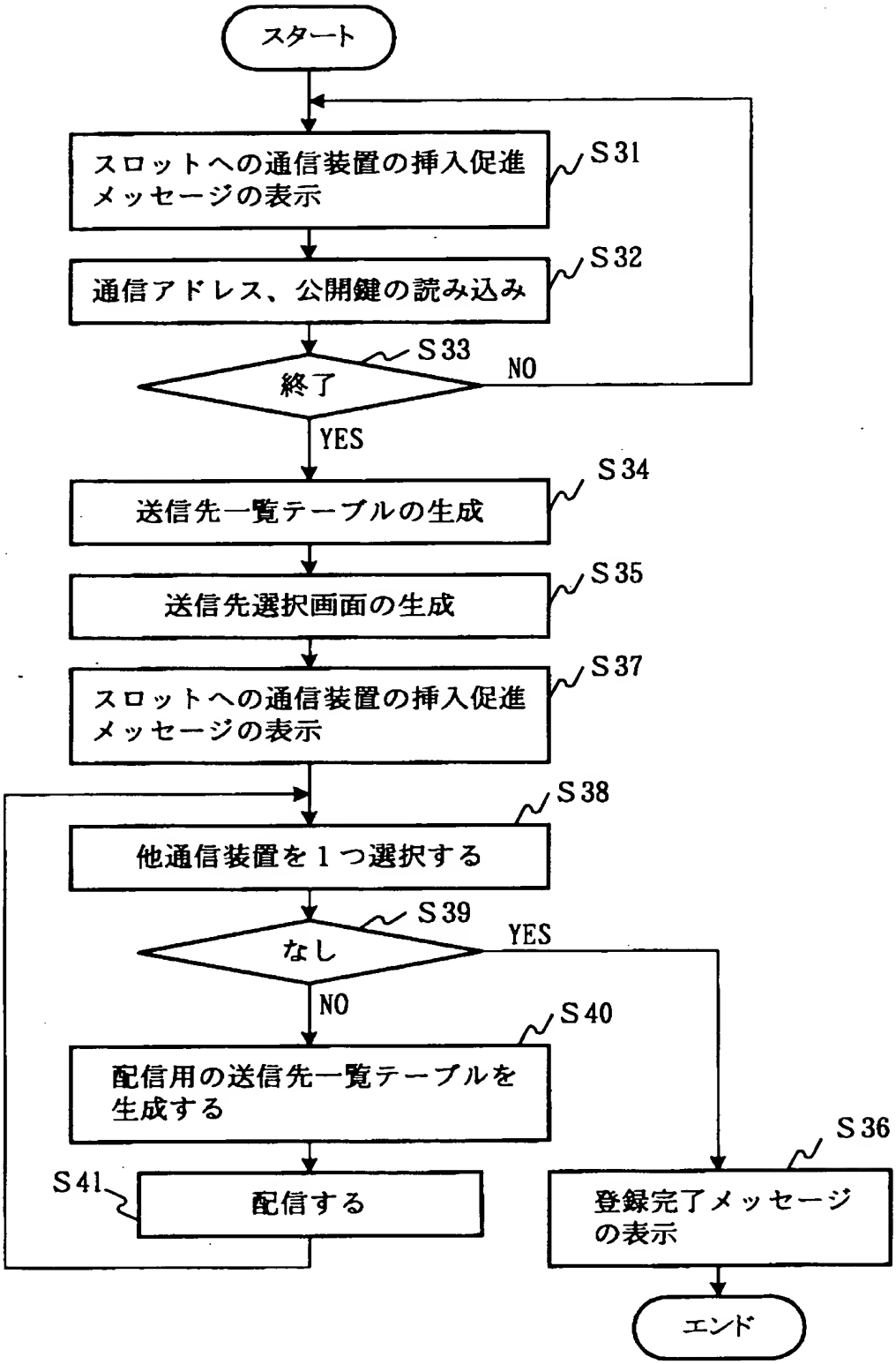
【図１２】


(a)
通信装置番号
通信アドレス
鍵
1
通信装置３ａの通信アドレス
通信装置３ａの秘密鍵
通信装置３ａの公開鍵
１４０
(b)
通信装置番号
通信アドレス
鍵
2
通信装置３ｂの通信アドレス
通信装置３ｂの公開鍵
3
通信装置３ｃの通信アドレス
通信装置３ｃの公開鍵
１４１
(c)
送信先は？
2 番
3 番
１４２

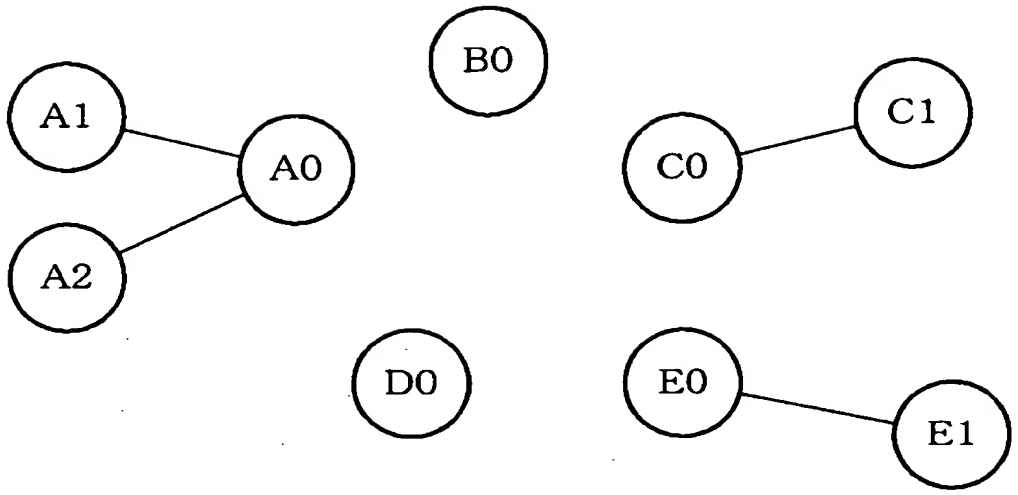
【図１３】


スタート
S31
スロットへの通信装置の挿入促進
メッセージの表示
S32
通信アドレス、公開鍵の読み込み
S33
終了
NO
YES
S34
送信先一覧テーブルの生成
S35
送信先選択画面の生成
S36
登録完了メッセージの表示
エンド

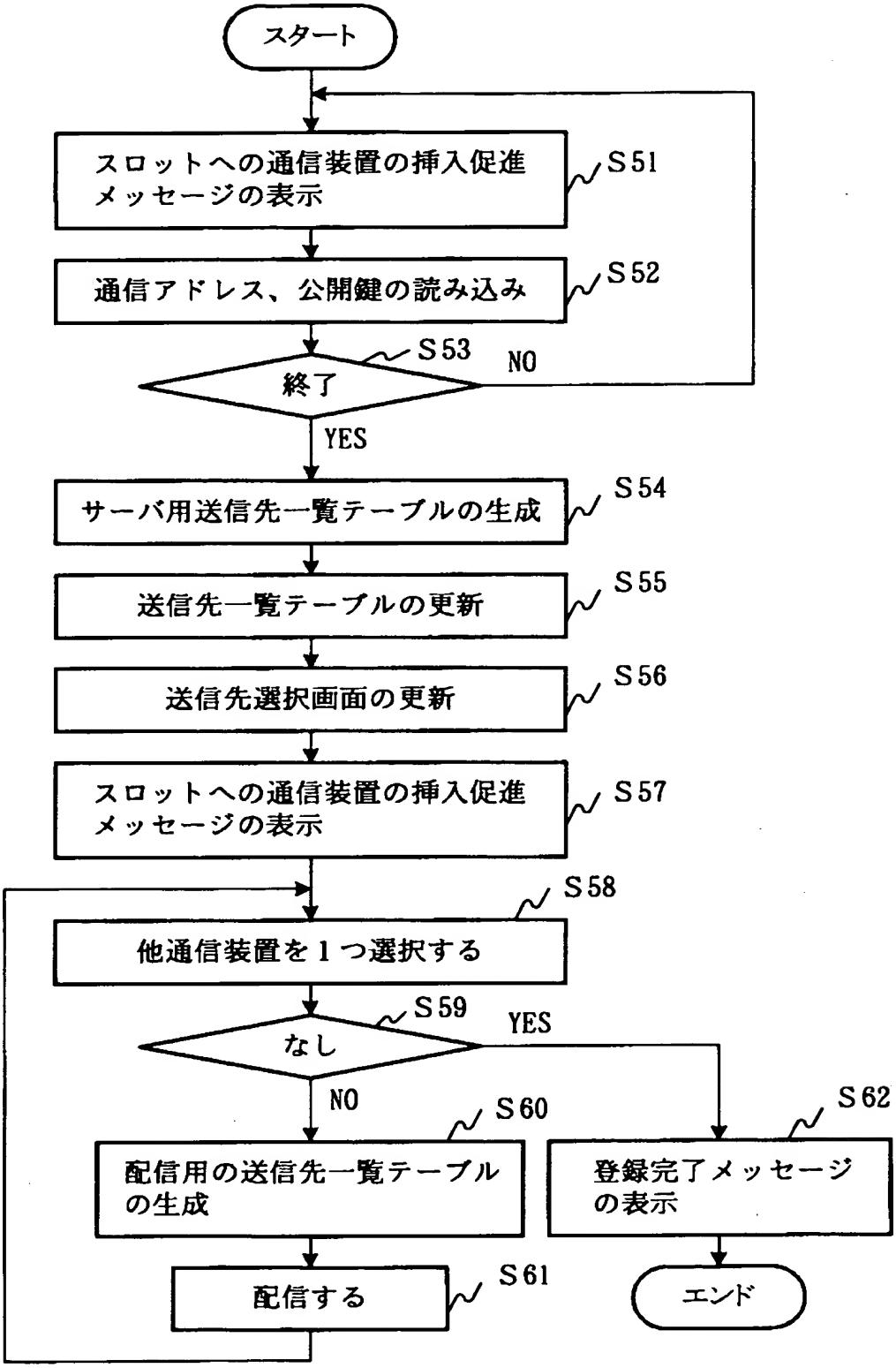
【図１４】


スタート
スロットへの通信装置の挿入促進メッセージの表示
S31
通信アドレス、公開鍵の読み込み
S32
終了
S33
NO
YES
送信先一覧テーブルの生成
S34
送信先選択画面の生成
S35
スロットへの通信装置の挿入促進メッセージの表示
S37
他通信装置を１つ選択する
S38
なし
S39
YES
NO
配信用の送信先一覧テーブルを生成する
S40
S41
配信する
登録完了メッセージの表示
S36
エンド

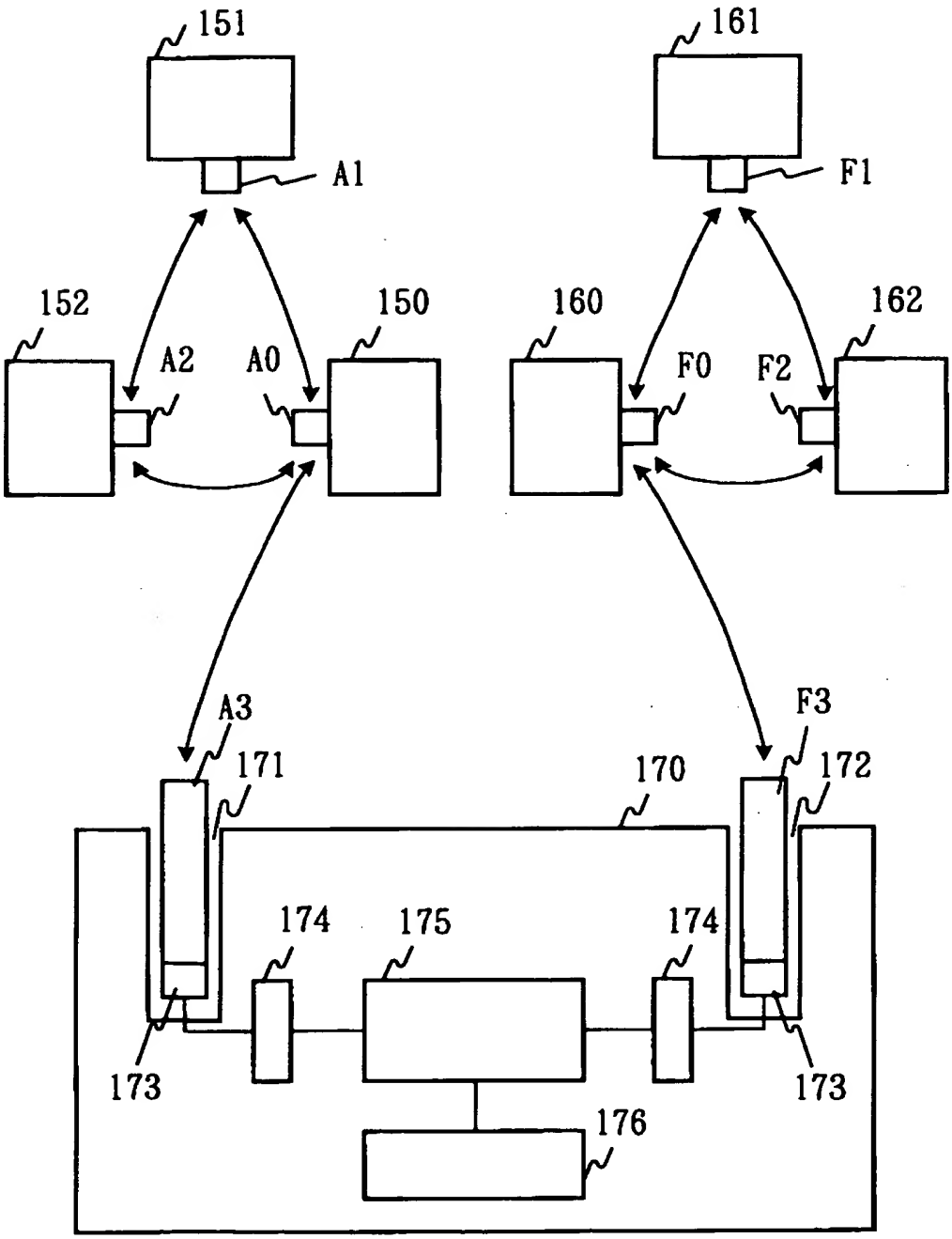
【図１５】



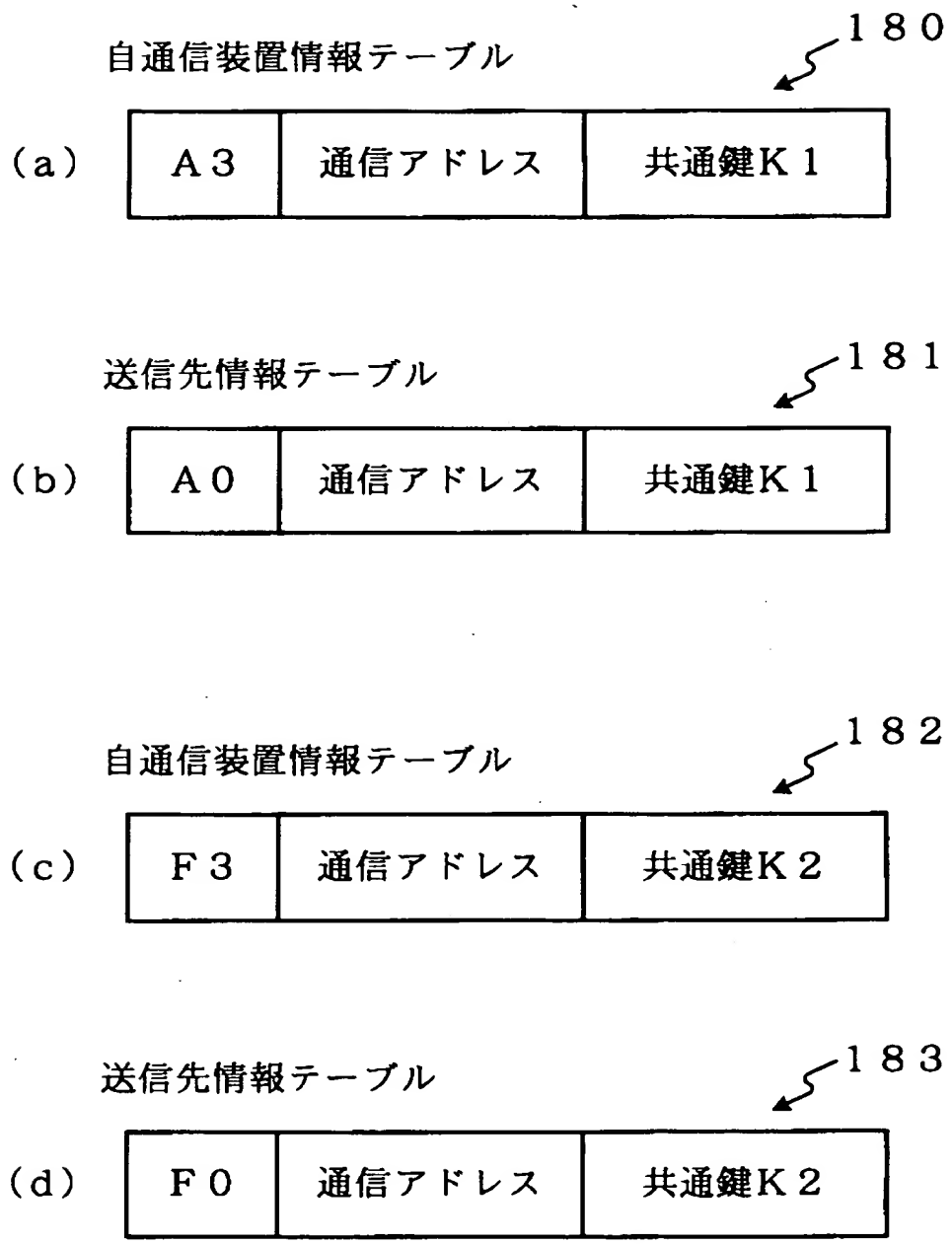
【図１６】


スタート
スロットへの通信装置の挿入促進メッセージの表示
S51
通信アドレス、公開鍵の読み込み
S52
S53
終了
NO
YES
サーバ用送信先一覧テーブルの生成
S54
送信先一覧テーブルの更新
S55
送信先選択画面の更新
S56
スロットへの通信装置の挿入促進メッセージの表示
S57
S58
他通信装置を１つ選択する
S59
なし
YES
NO
S60
配信用の送信先一覧テーブルの生成
S62
登録完了メッセージの表示
配信する
S61
エンド

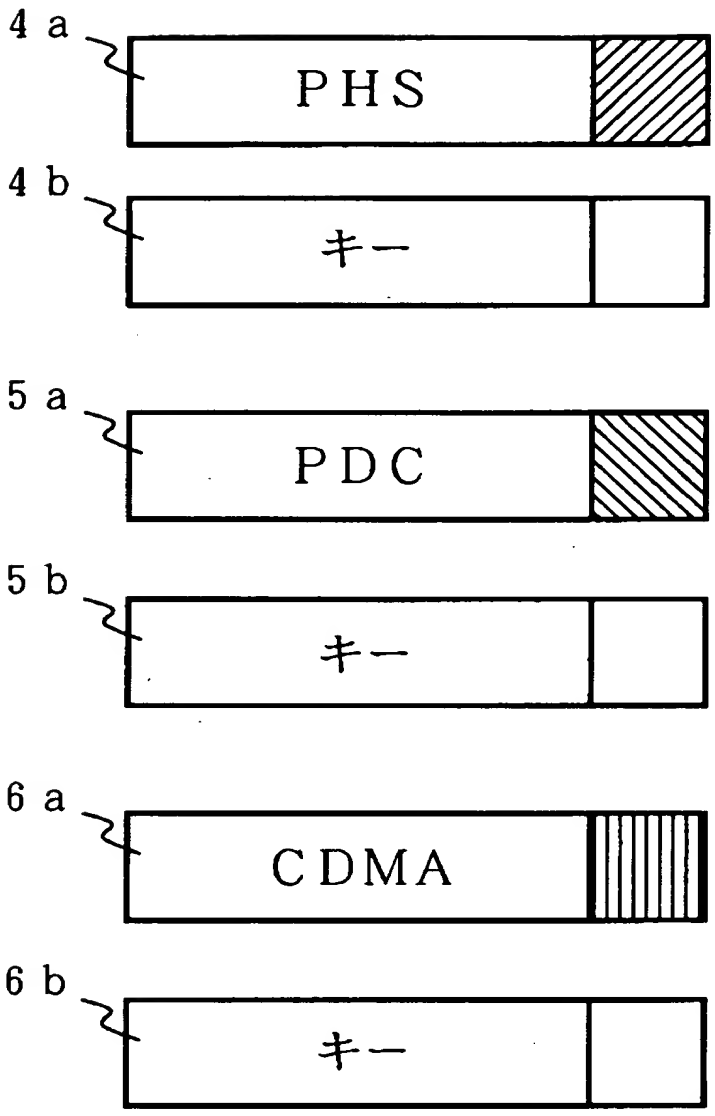
【図１７】


151
161
A1
F1
152
150
160
162
A2
A0
F0
F2
A3
F3
171
170
172
174
175
174
173
173
176

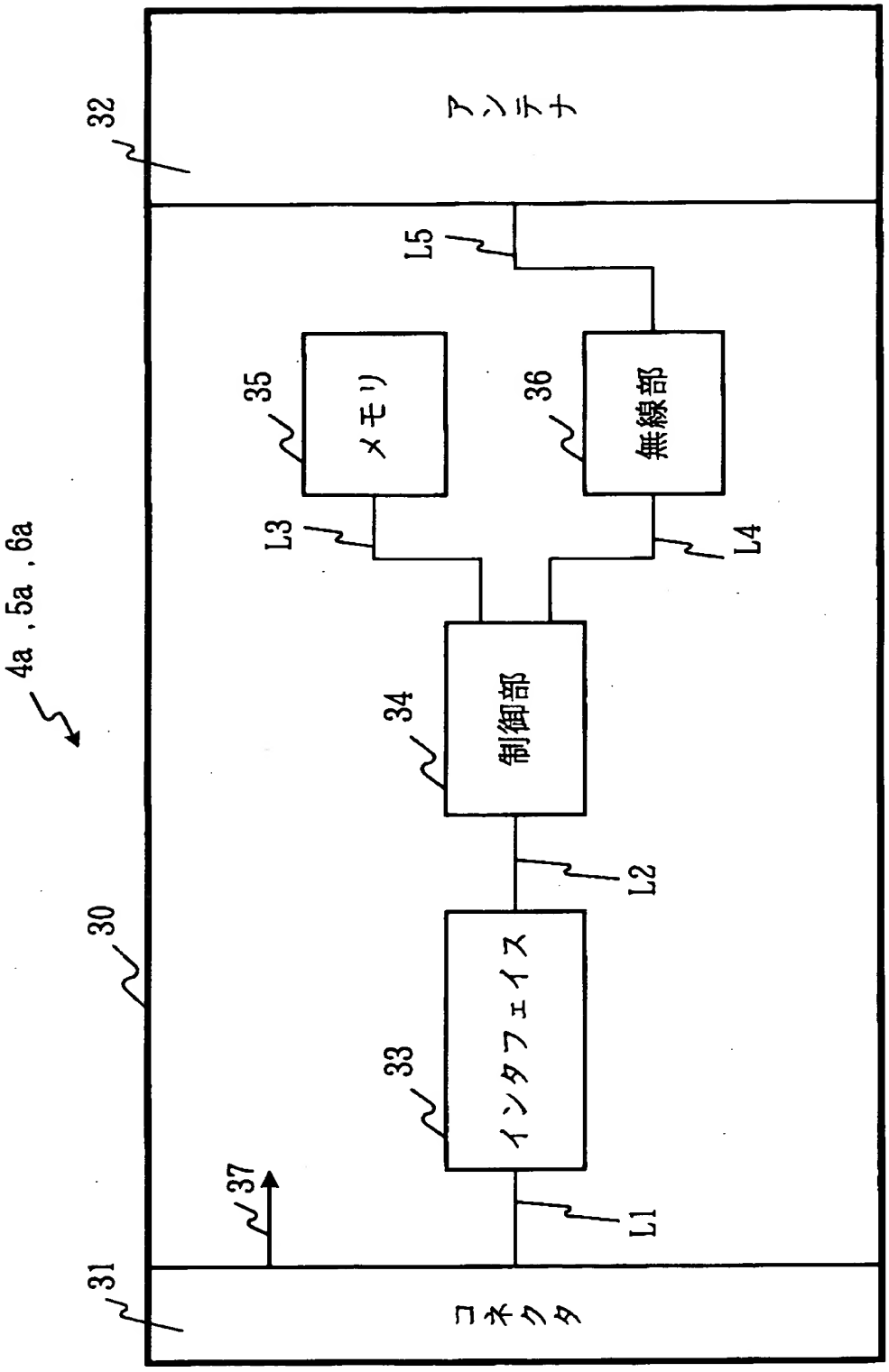
【図１８】


自通信装置情報テーブル
１８０
（a）
Ａ３
通信アドレス
共通鍵Ｋ１
送信先情報テーブル
１８１
（b）
Ａ０
通信アドレス
共通鍵Ｋ１
自通信装置情報テーブル
１８２
（c）
Ｆ３
通信アドレス
共通鍵Ｋ２
送信先情報テーブル
１８３
（d）
Ｆ０
通信アドレス
共通鍵Ｋ２

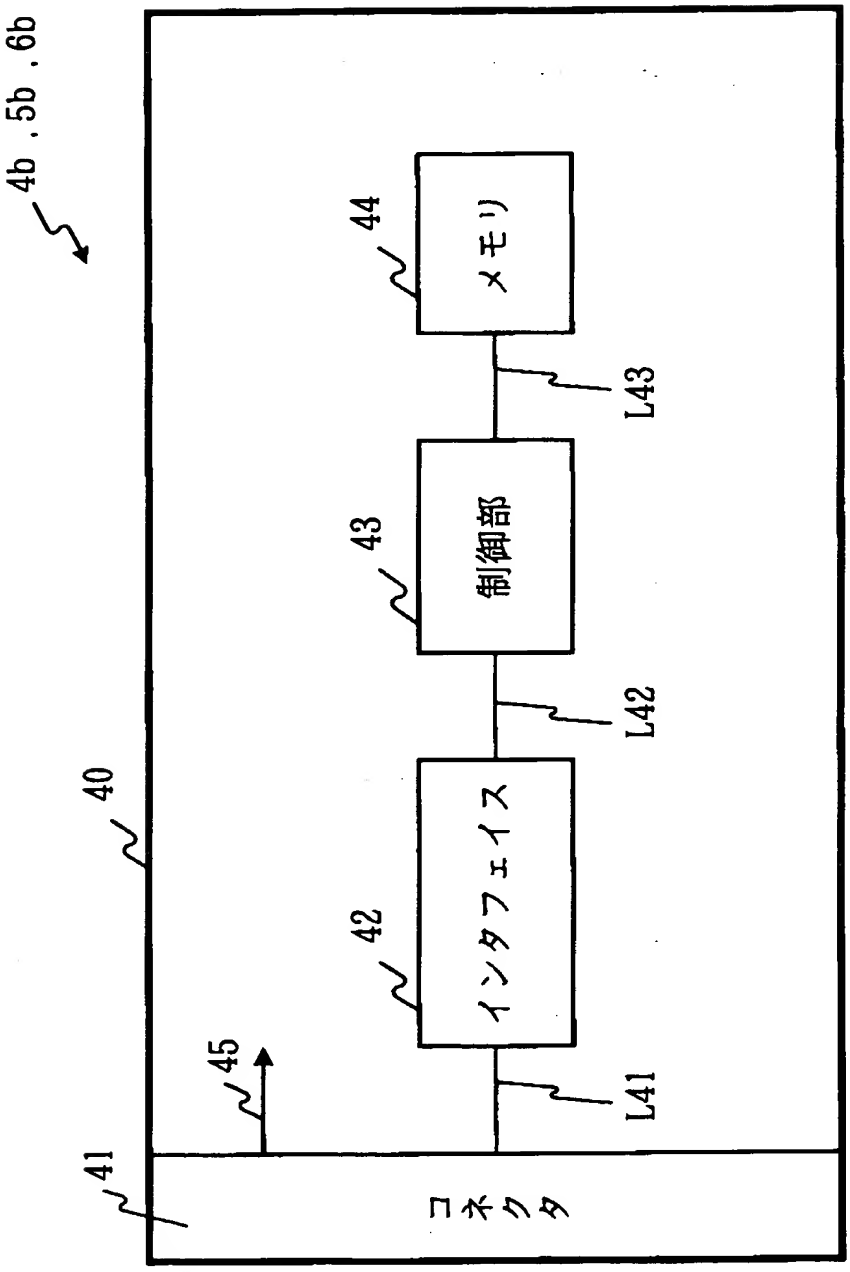
【図１９】



【図２０】

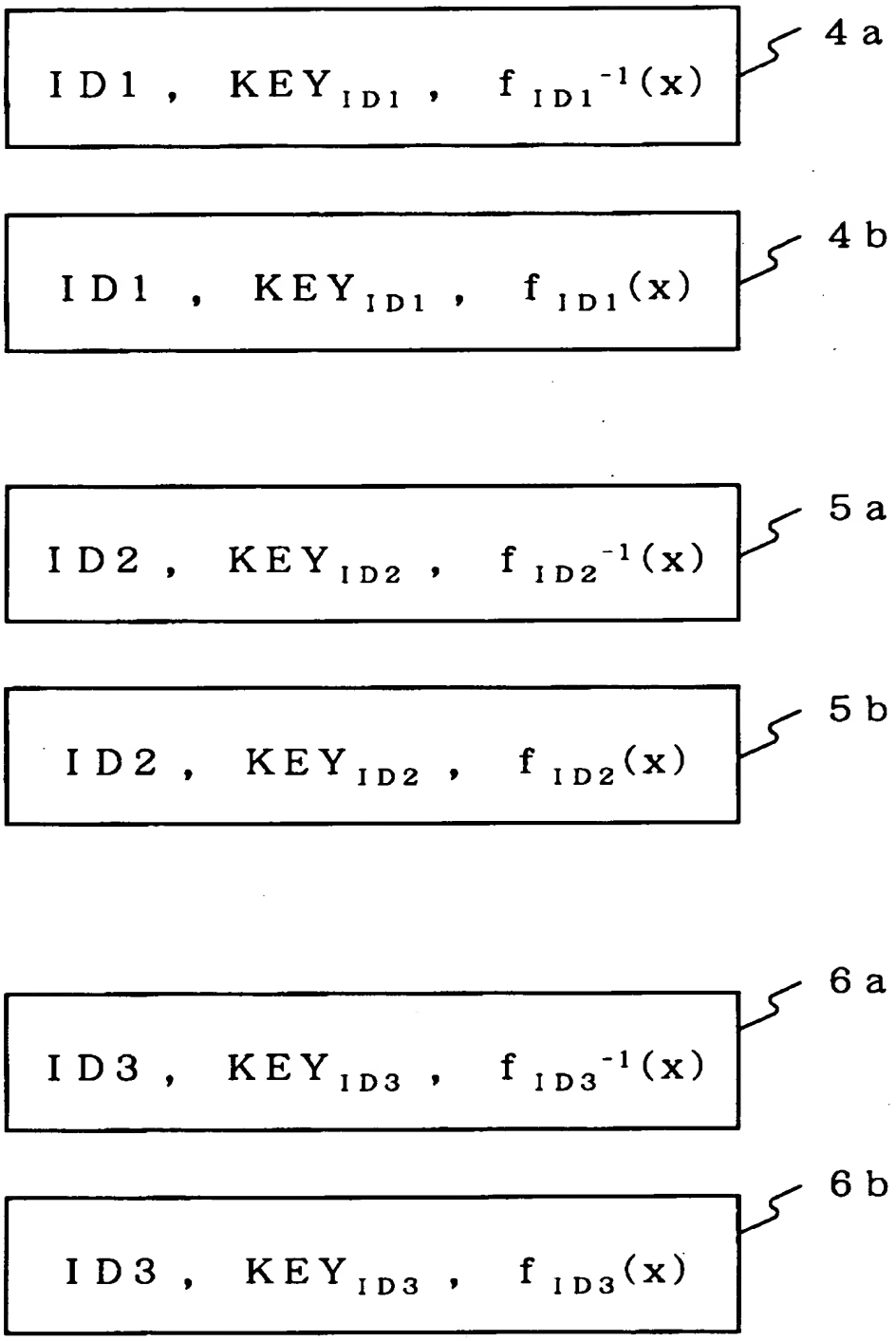

4a , 5a , 6a
32
アンテナ
L5
35
メモリ
36
無線部
L3
L4
34
制御部
L2
30
33
インタフェイス
37
L1
31
コネクタ

【図２１】

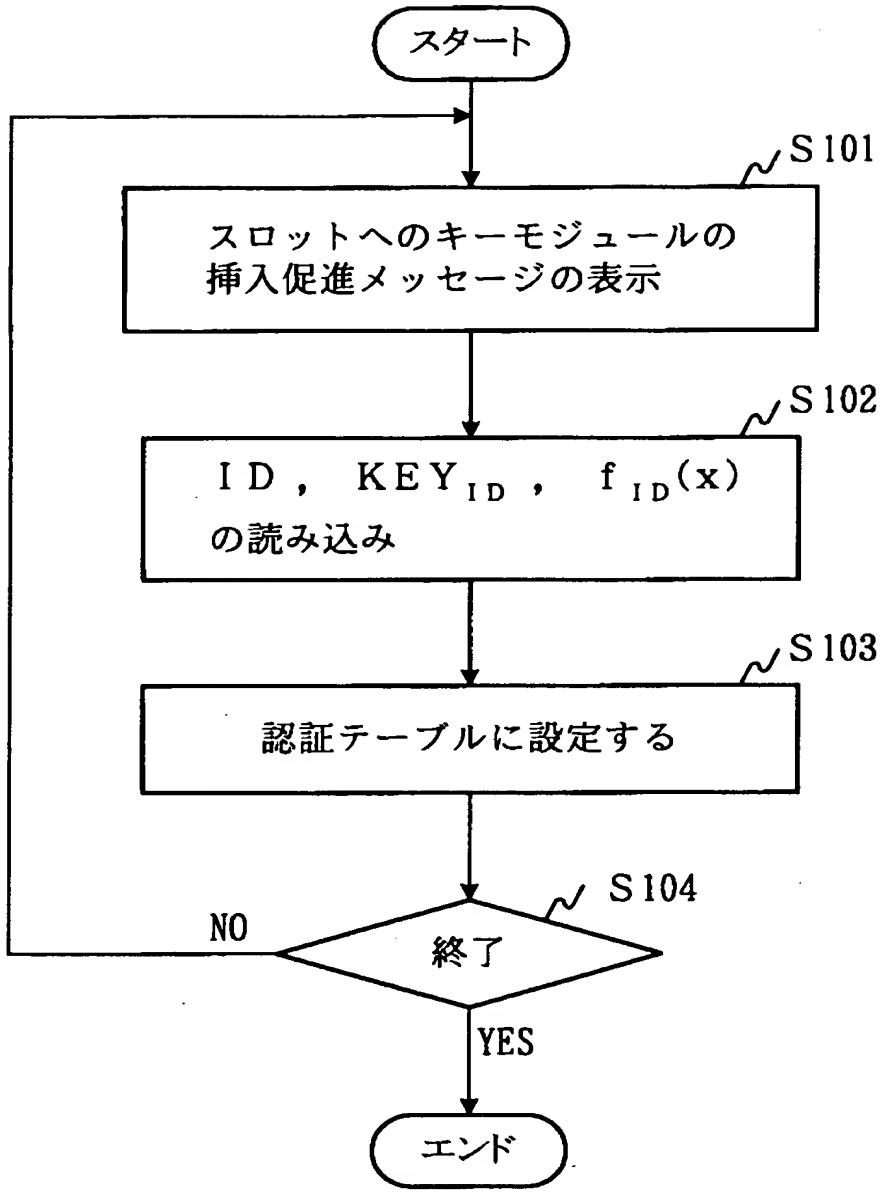


出証特２０００－３０７２０９４

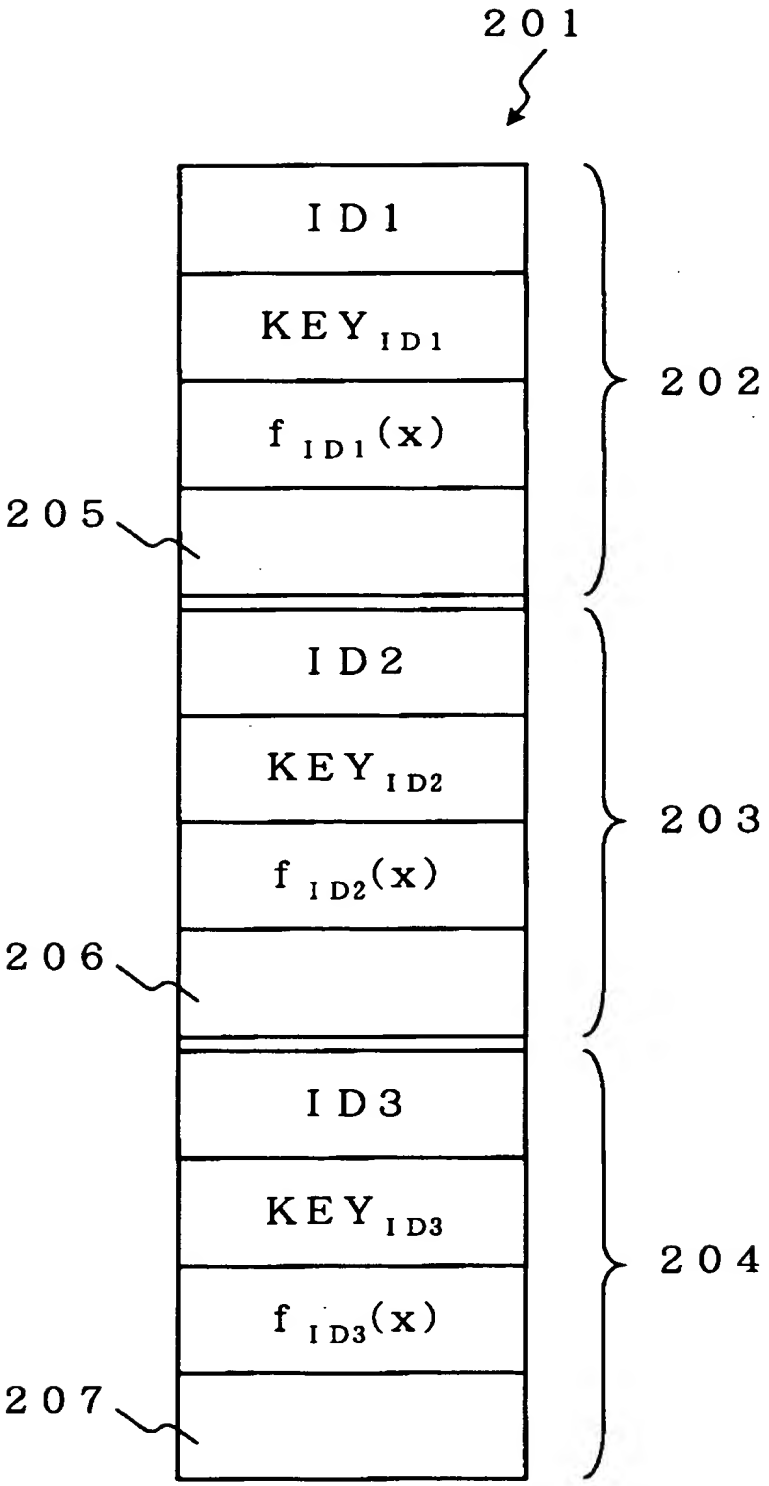
【図２２】


ID1 , KEY$_{ID1}$, $f_{ID1}^{-1}(x)$
4a
ID1 , KEY$_{ID1}$, $f_{ID1}(x)$
4b
ID2 , KEY$_{ID2}$, $f_{ID2}^{-1}(x)$
5a
ID2 , KEY$_{ID2}$, $f_{ID2}(x)$
5b
ID3 , KEY$_{ID3}$, $f_{ID3}^{-1}(x)$
6a
ID3 , KEY$_{ID3}$, $f_{ID3}(x)$
6b

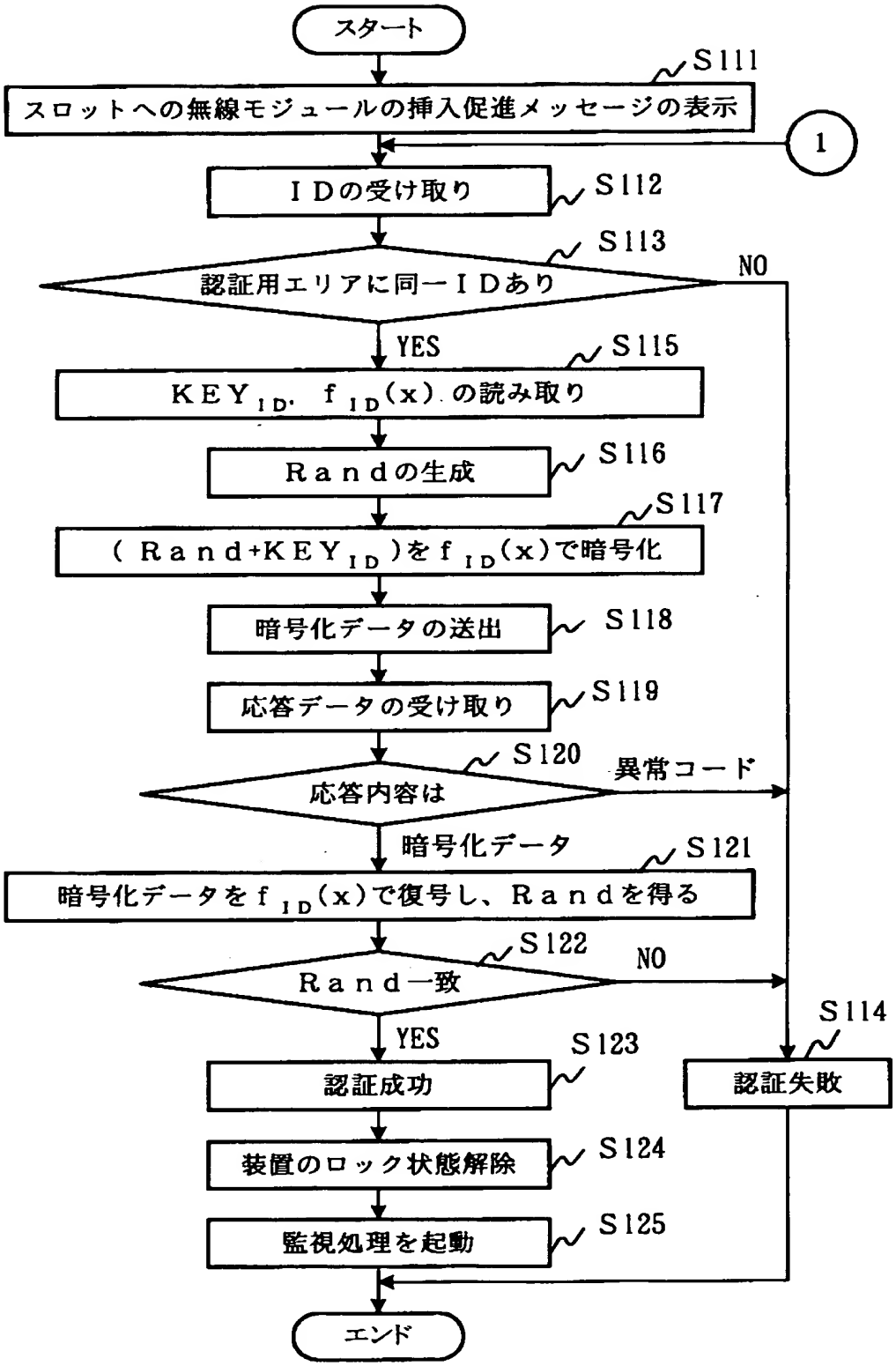
【図２３】


スタート
S101
スロットへのキーモジュールの
挿入促進メッセージの表示
S102
ＩＤ，　KEY_{ID}，　$f_{ID}(x)$
の読み込み
S103
認証テーブルに設定する
S104
NO
終了
YES
エンド

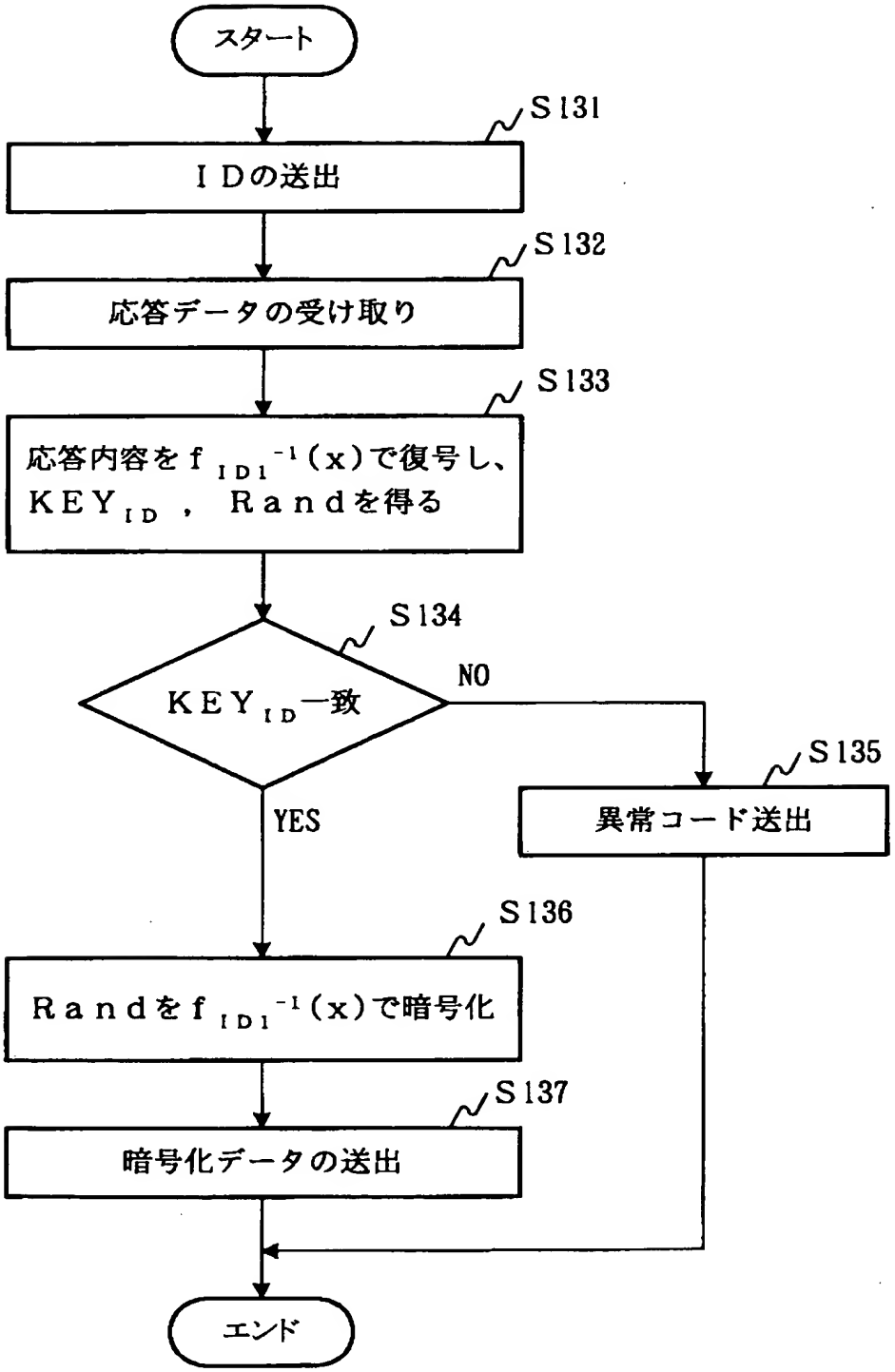
【図２４】


２０１
ＩＤ１
KEY ID1
f ID1(x)
２０５
２０２
ＩＤ２
KEY ID2
f ID2(x)
２０６
２０３
ＩＤ３
KEY ID3
f ID3(x)
２０７
２０４

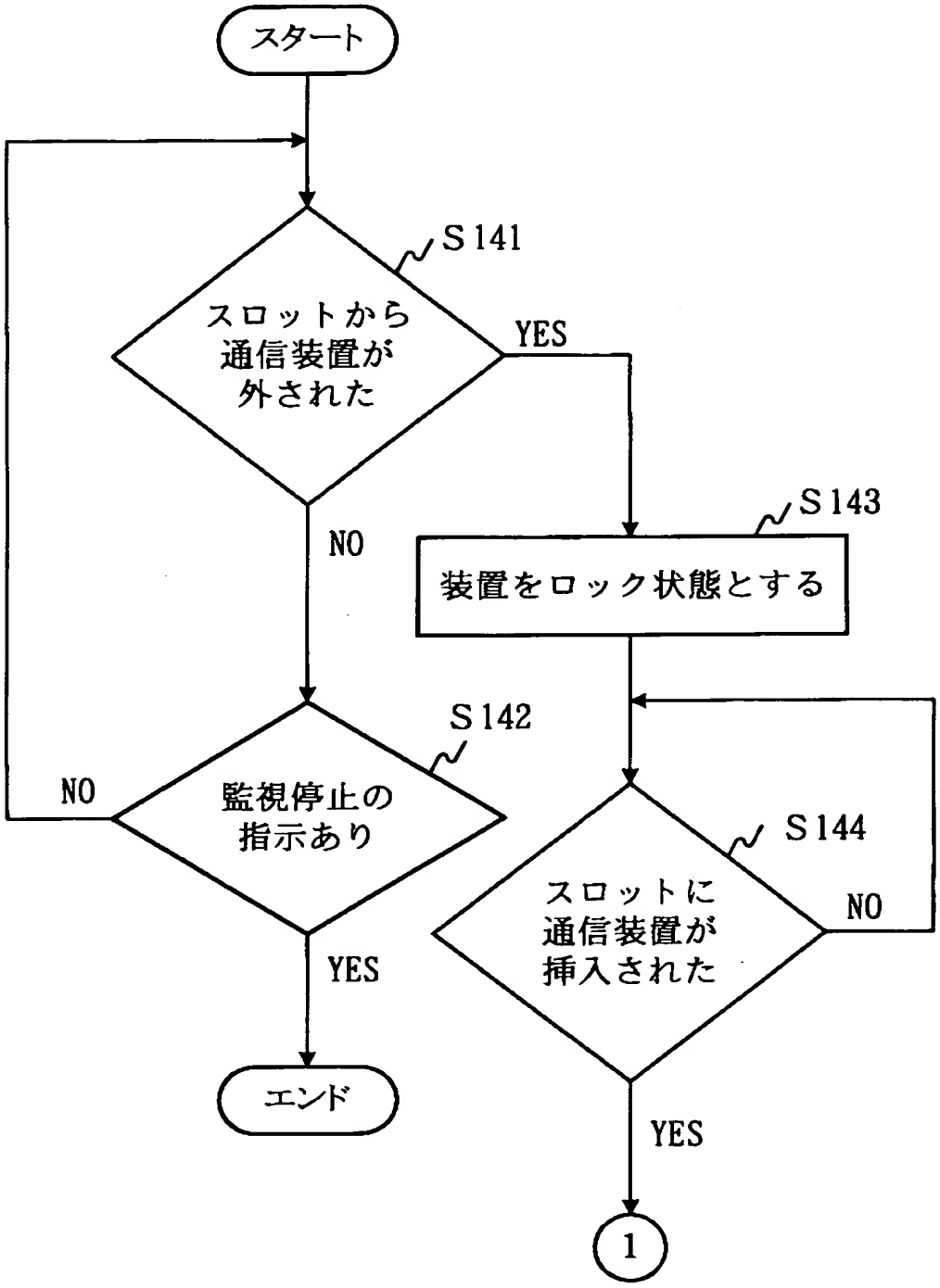
【図２５】


スタート
S111
スロットへの無線モジュールの挿入促進メッセージの表示
1
ＩＤの受け取り
S112
S113
認証用エリアに同一ＩＤあり
NO
YES
S115
KEY_{ID}, $f_{ID}(x)$ の読み取り
Ｒａｎｄの生成
S116
S117
(Ｒａｎｄ+KEY_{ID})を $f_{ID}(x)$ で暗号化
暗号化データの送出
S118
応答データの受け取り
S119
S120
応答内容は
異常コード
暗号化データ
S121
暗号化データを $f_{ID}(x)$ で復号し、Ｒａｎｄを得る
S122
Ｒａｎｄ一致
NO
YES
S123
認証成功
S114
認証失敗
装置のロック状態解除
S124
監視処理を起動
S125
エンド

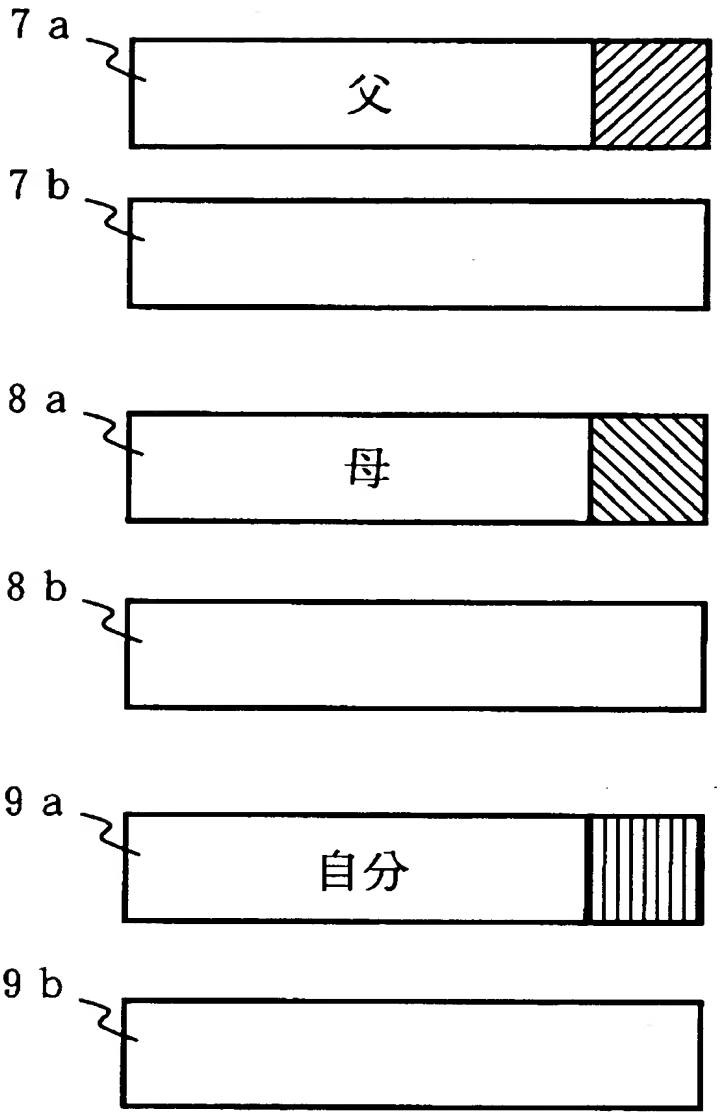
【図２６】


スタート
S131
ＩＤの送出
S132
応答データの受け取り
S133
応答内容を$f_{ID1}^{-1}(x)$で復号し、
KEY_{ID}，Ｒａｎｄを得る
S134
KEY_{ID}一致
NO
YES
S135
異常コード送出
S136
Ｒａｎｄを$f_{ID1}^{-1}(x)$で暗号化
S137
暗号化データの送出
エンド

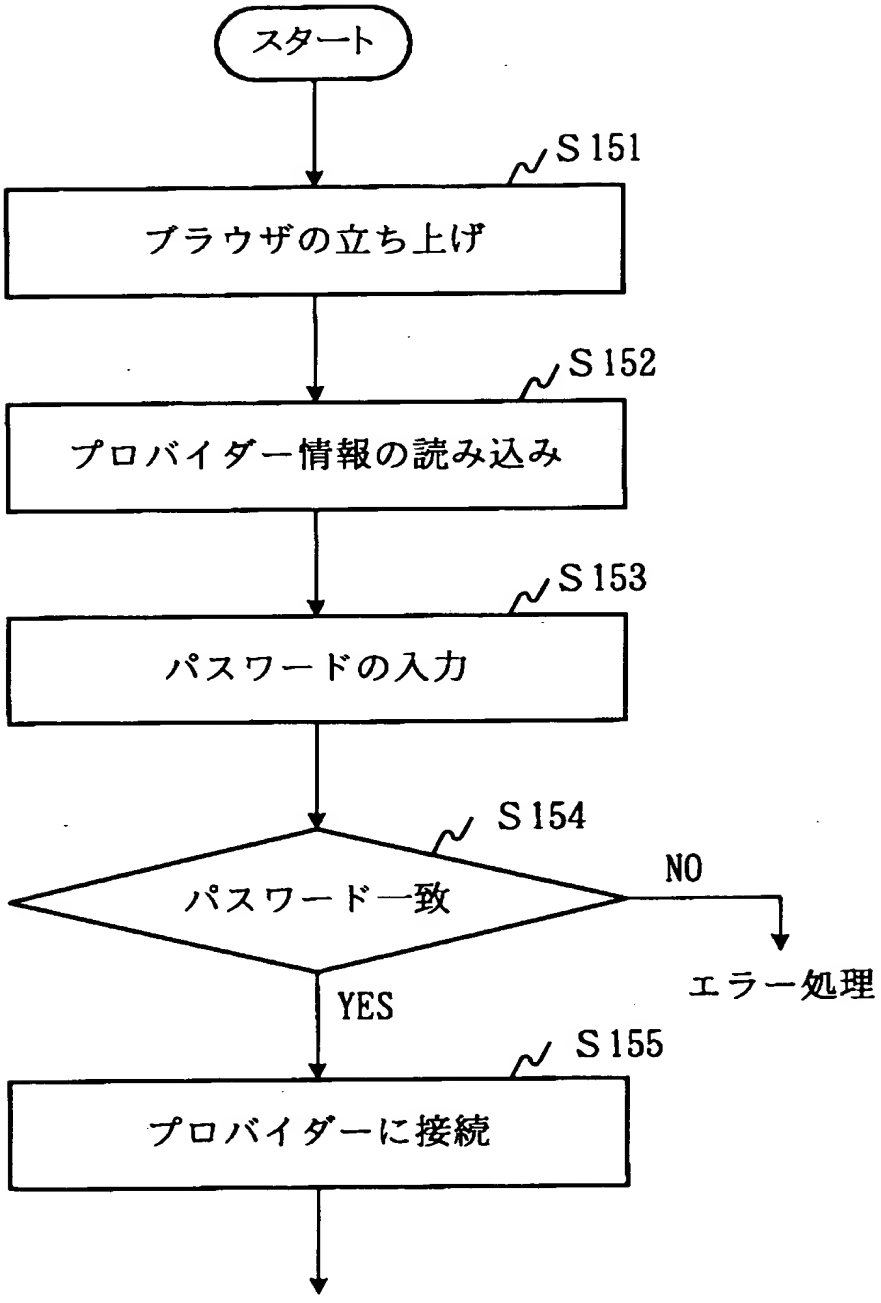
【図２７】


スタート
S141
スロットから
通信装置が
外された
YES
NO
S143
装置をロック状態とする
S142
監視停止の
指示あり
NO
S144
スロットに
通信装置が
挿入された
NO
YES
エンド
YES
1

【図２８】



【図２９】



出証特２０００－３０７２０９４

【書類名】　　要約書

【要約】

【課題】　端末装置どうしを手軽にワイヤレス接続できるようにする。

【解決手段】　通信装置3a～3cのセットは規格化された形状を有する。端末1a～1cをワイヤレス接続する場合、通信装置3b、3cを端末1aのスロット2aに挿入し、通信装置3b、3cに記憶された通信アドレス及びセット固有の共通鍵を端末1aに登録する。同様に端末1bに通信装置3a、3cの、端末1cに通信装置3a、3bの、通信アドレス及びセット固有の共通鍵を登録する。その後、端末1aに通信装置3aを、端末1bに通信装置3bを、端末1cに通信装置3cをそれぞれ挿入し、送信先アドレス及び送信元アドレスに送信先通信装置および送信元通信装置の通信アドレスを使用し、送信データの暗号化及び復号に共通鍵を使用し、端末1a～1c間でデータを送受信する。通信装置3a～3cは端末からはみ出る部分が伝送速度に応じた色で色付けされており、色を見れば通信装置セットの種類が判別できる。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４２３７〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　　東京都港区芝五丁目７番１号
氏　名　　日本電気株式会社